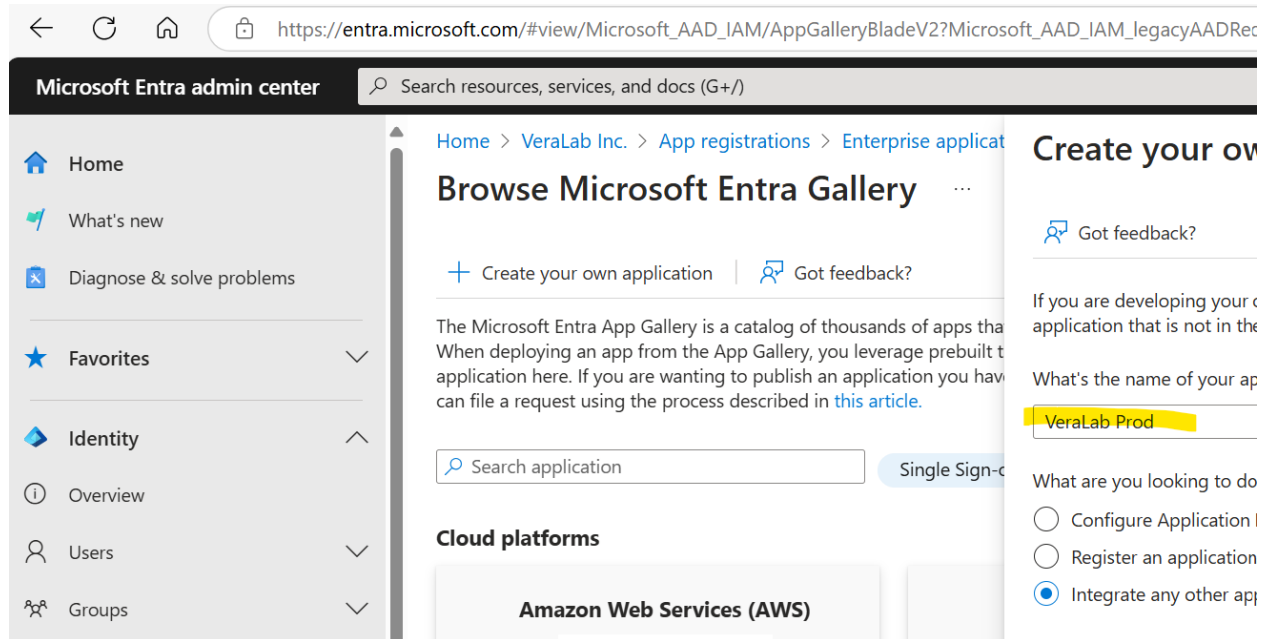


VERALAB SSO Integration with Microsoft Azure SAML

1. Login to your Microsoft Entra Admin Center page and go to Identity -> Enterprise Applications -> Create your own application. Give it a name, e.g. VeraLab Test or VeraLab Prod depending on your environment. Keep default "Integrate any other application..." option and click "Create" button in the bottom.



2. On the Overview page click on "Get started" under Set up single sign on block.

Home > VeraLab Inc. > App registrations > Enterprise applications | All applications > Browse Microsoft Entra Gallery >

VeraLab Prod | Overview

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Properties

VP

Name ⓘ

VeraLab Prod


Application ID ⓘ


16981ef3-dd84-4dbe-85db...

Object ID ⓘ

dfbd106a-ca0b-40a1-b3ae...

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. Click on SAML block.

VeraLab Prod | Single sign-on

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service
- Custom security attributes

Security

- Conditional Access
- Permissions
- Token encryption

Single sign-on (SSO) adds security and convenience when users sign on to an application. When you enable SSO for an application, you can enable a user in your organization to sign in to every application they use. When a user signs into an application, that credential is used for all the other applications that the user can access.

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.

- From the Setup Page, copy App Federation Metadata URL:

3

SAML Certificates

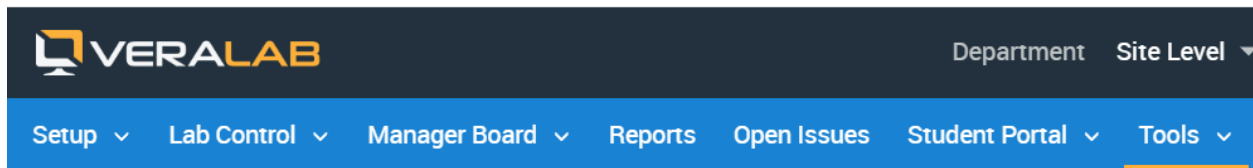
Token signing certificate

[Edit](#)

Status	Active
Thumbprint	DCF68AE047F204D42EDC2B6362C6B7626850E44D
Expiration	9/26/2029, 12:27:27 PM
Notification Email	[REDACTED]@veralab.com
App Federation Metadata Url	https://login.microsoftonline.com/bfe332c...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

- Login to VeraLab Web Application as a user with Administrator role. If you have Enterprise Edition license, change **Department** to **Site Level**.

- Go to **Tools -> Settings -> Single Sign-on Settings**. Select **Enable an additional authentication method** checkbox and click **Save**.



Single Sign-on Settings

Please note: Enabling Single Sign-On (SSO) will deactivate the ability to log into the web application via LDAP. All current LDAP accounts will be automatically converted to SSO accounts and will only be usable through the Single Sign-On mechanism. Conversely, disabling Single Sign-On will convert all SSO accounts back to LDAP accounts.

Set sign-on options for users accessing VeraLab

☒ Enable an additional authentication method

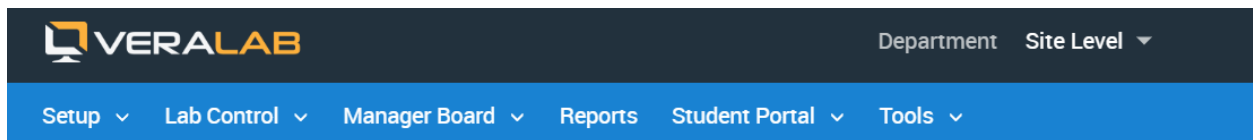
Authentication *

SAML

Save

Cancel

- On the SAML Authentication Settings verify that Hostname and port are equal to your VeraLab application FQDN, e.g. if you registered VeraLab on your campus DNS server, it may look like `veralab.myuniversity.edu` and 443 for hostname and port number accordingly.



SAML Authentication Settings

To ensure the correct functioning of Single Sign-On, it is necessary to enable HTTPS support. Additionally, you must specify the hostname and HTTPS port on which VeraLab is operating. Responses from the authentication server will be redirected to this address.

Hostname *

veralab.myuniversity.edu

Port *

443

- Click on **Import Settings from IdP Metadata** and paste "App Federation Metadata URL" from IDP. Click **Import** button.

Import Settings from IdP Metadata

☒ Import from URL

<https://login.microsoftonline.com/bfe332c8-f9cf-462b-9708-b623a8054277>

☐ Import from file


Choose File No file chosen

☐ Import from text below

Import

Close

9. Click Save leaving other settings default.
10. Export VeraLab Metadata and save it as XML file.

 VERALAB

Department Site Level ▾

Setup ▾ Lab Control ▾ Manager Board ▾ Reports Student Portal ▾ Tools ▾

Single Sign-on Settings

Set sign-on options for users accessing VeraLab

☒ Enable an additional authentication method

Authentication *

SAML ▾

SAML Settings

Export metadata from VeraLab SP

Choose a method for sharing VeraLab SP metadata with your IdP.

Method 1: Export metadata

Export a metadata (.xml) file.

Export metadata

11. Go back to IDP Entra admin center and click on Upload metadata file.

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Home > VeraLab Inc. > App registrations > Enterprise applications | All applications > Browse Microsoft En

VeraLab Prod | SAML-based Sign-on

Enterprise Application

Overview Deployment Plan Diagnose and solve problems

Manage Properties Owners Roles and administrators Users and groups Single sign-on Provisioning Application proxy Self-service

Upload metadata file Change single sign-on mode Test this application Got feedback?

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security and is easier to implement. Choose SAML single sign-on whenever possible for Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating VeraLab Prod.

- 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
- Advanced SAML Configuration

12. Select XML file you saved from VeraLab and click **Add** button.

Upload metadata file.

Values for the fields below are provided by VeraLab Prod. You may either enter those values manually, or use a pre-configured SAML metadata file if provided by VeraLab Prod.

"VL_SP_Metadata.xml"

Add Cancel

13. Click **Save** to complete metadata upload.

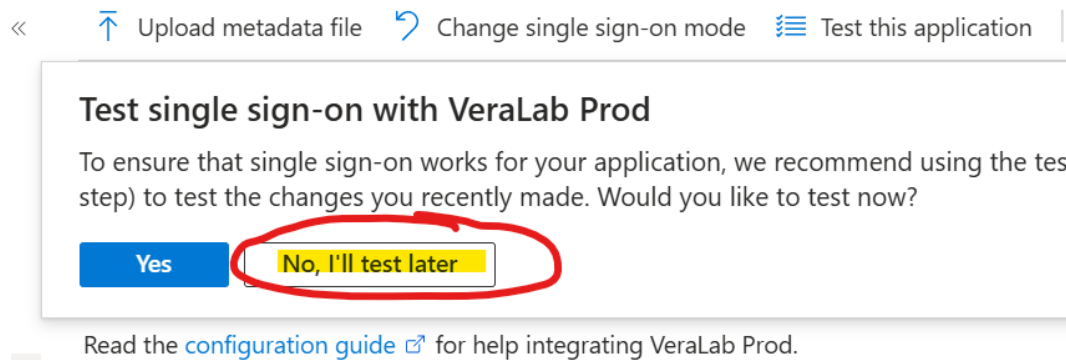
Basic SAML Configuration

Save Got feedback?

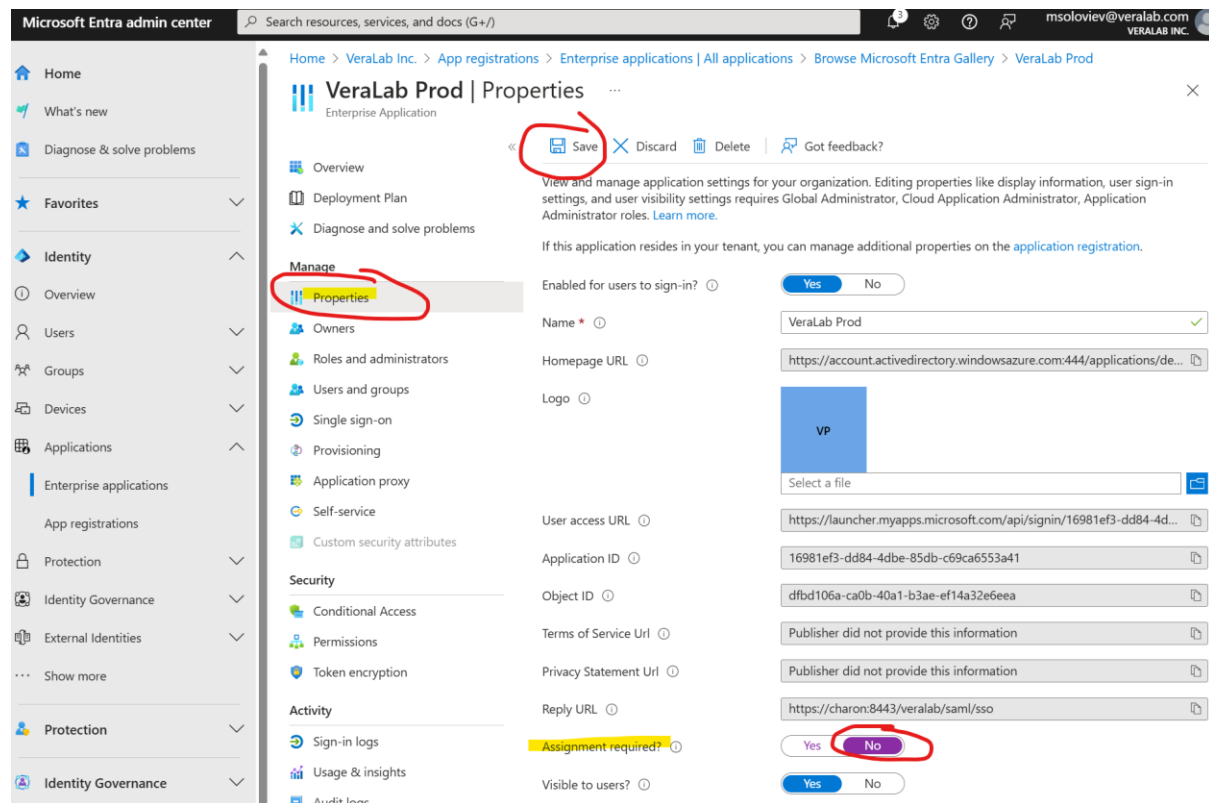
Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique to your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for

14. Click **No, I'll test later** button on the next screen.



15. Go to Properties screen, update “Assignment required” attribute to “No” and click Save.






16. Go to Single Sign On screen and edit Attributes & Claims. Delete or edit existing Additional claims using below three mappings email=user.mail, first_name=user.givenname, last_name=user.surname. Namespace attribute can be set to blank.

Additional claims

Claim name	Type	Value	
email	SAML	user.mail	...
first_name	SAML	user.givenname	...
last_name	SAML	user.surname	...

Manage claim ...

 Save  Discard changes |  Got feedback?

Name *

first_name

Namespace

Enter a namespace URI

Choose name format

Source *

☒ Attribute ☐ Transformation ☐ Directory schema extension

Source attribute *

user.givenname

Claim conditions







Advanced SAML claims options




17. Test SSO Integration using “Test this application” link.

... > [SAML-based Sign-on](#) > [Attributes & Claims](#) > [Diagnose and solve problems](#) > [Enterprise applications | All applications](#) >

VeraLab Prod | SAML-based Sign-on ...

Enterprise Application

-  Overview
-  Deployment Plan
-  Diagnose and solve problems
- Manage**
-  Properties
-  Owners
-  Roles and administrators

«  Upload metadata file  Change single sign-on mode  Test this application |

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experience. Choose SAML single sign-on whenever possible for existing applications. Connect or OAuth. [Learn more](#).

Read the [configuration guide](#)  for help integrating VeraLab Prod.

1 Basic SAML Configuration