

Reviewed by: Don Weobong

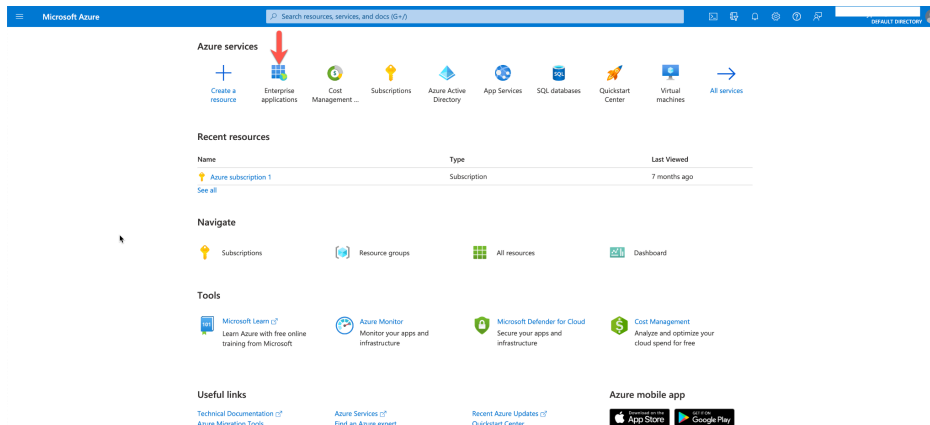
Review Date: 01-27-2026

Document # LSA-02

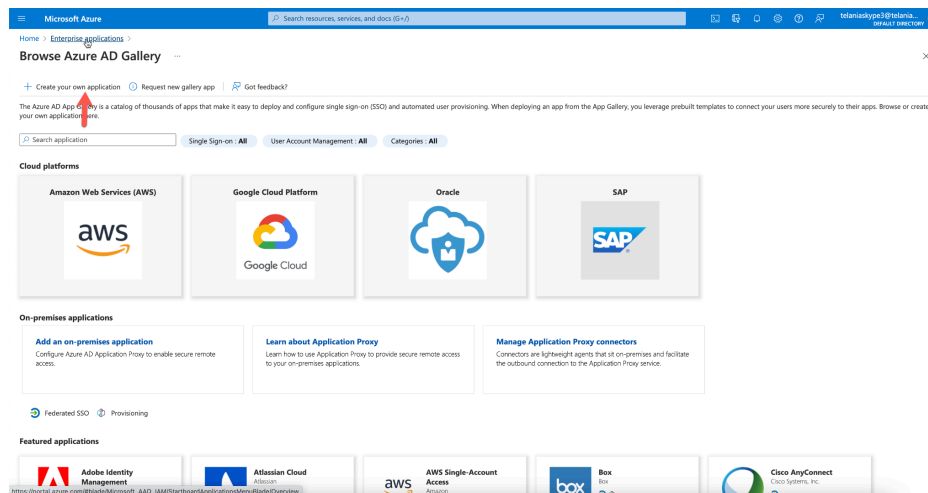
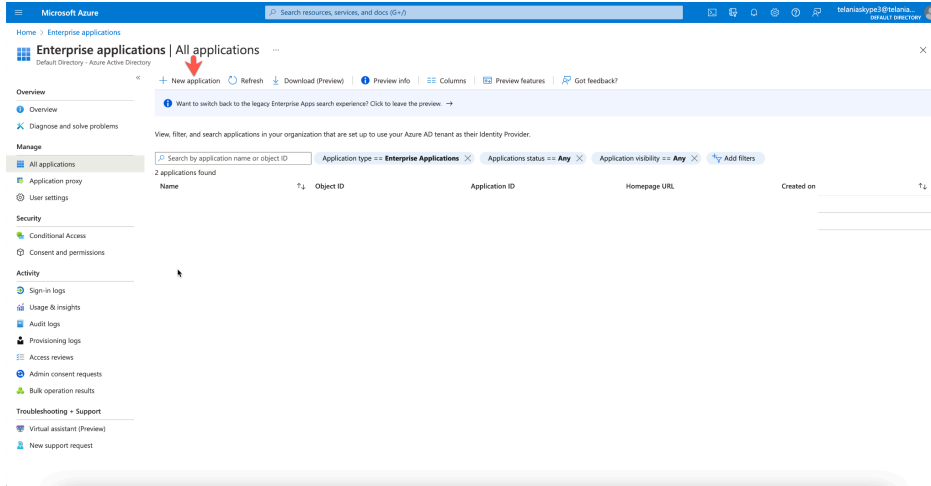
Version # 2.0

eLeaP LMS SAML 2.0 Azure Configuration

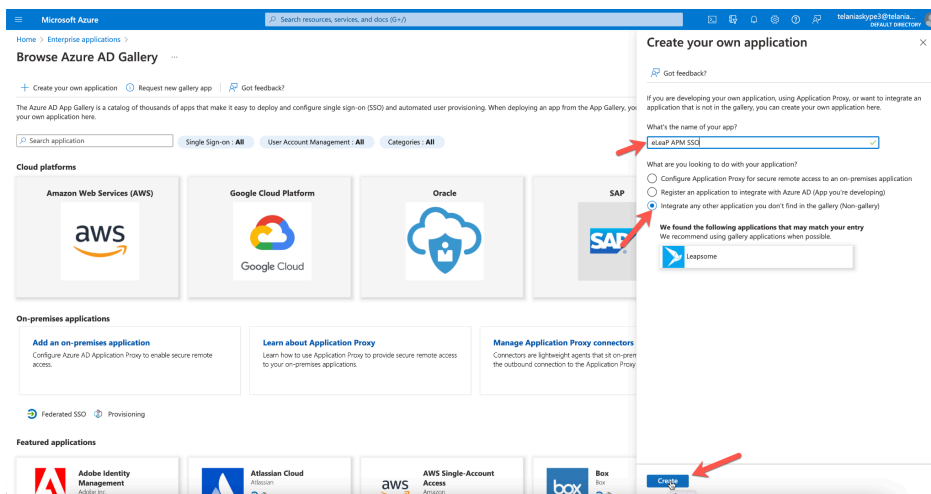
1. Go to Azure AD
2. Go to Enterprise apps



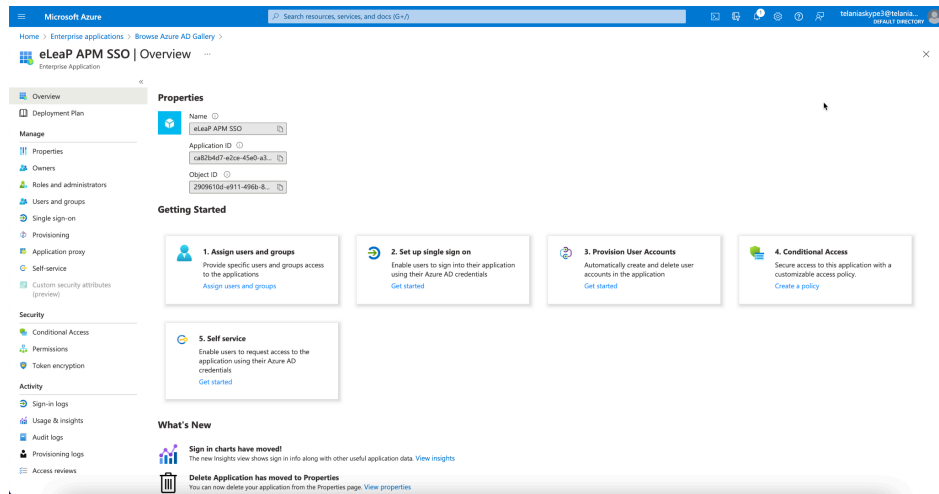
3. Create New Application



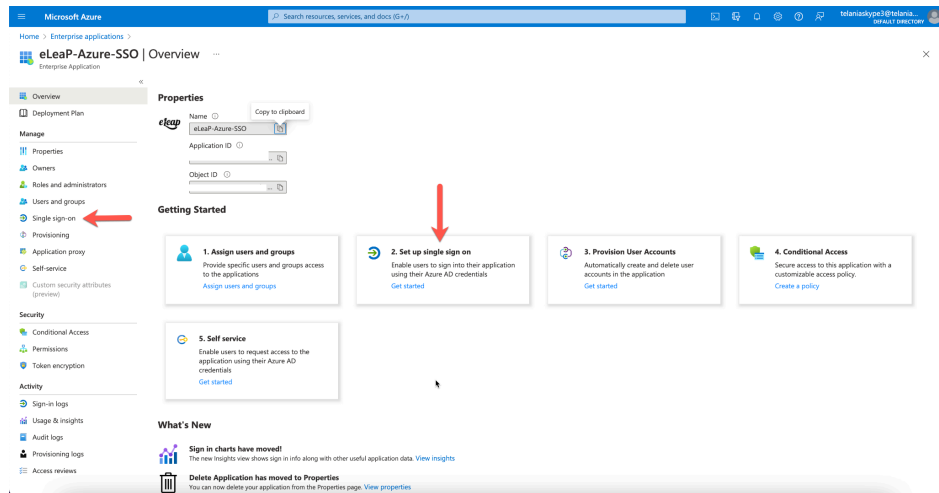
4. Non-gallery app



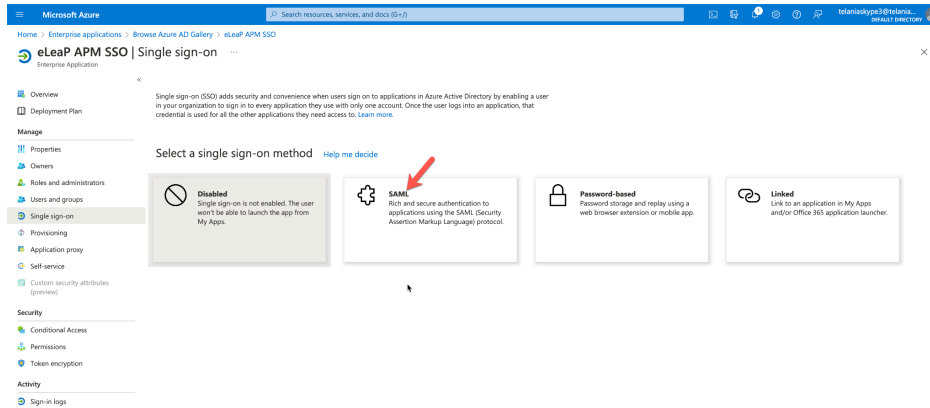
5. Set the name



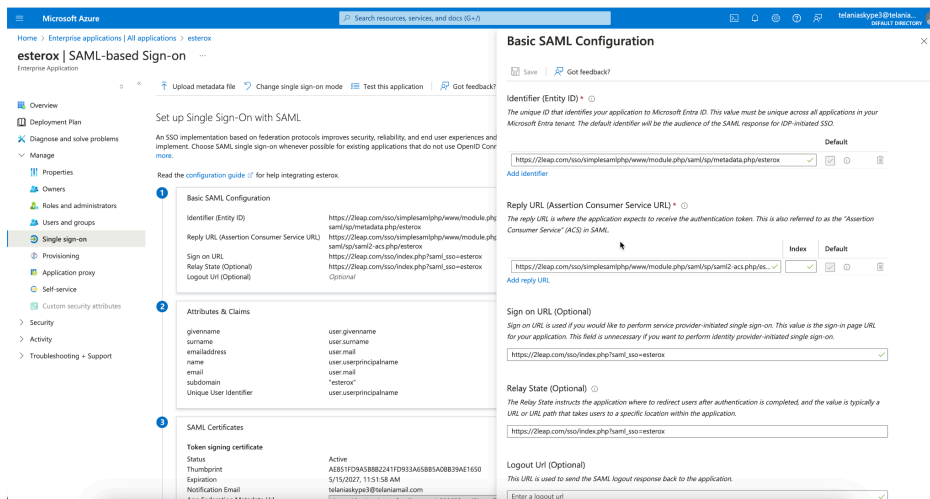
6. Go to SSO Settings



7. Set mode to SAML based SSO



8. Set App Domain and URLs Identifier:



Identifier: <https://2leap.com/sso/simplesamlphp/public/module.php/saml/sp/metadata.php/COMPANYSUBDOMAIN>
 Reply url: <https://2leap.com/sso/simplesamlphp/public/module.php/saml/sp/saml2-acss.php/COMPANYSUBDOMAIN>
 Sign on url: https://2leap.com/sso/index.php?saml_sso=COMPANYSUBDOMAIN
 Relay state: https://2leap.com/sso/index.php?saml_sso=COMPANYSUBDOMAIN
 Where COMPANYSUBDOMAIN is your eleap subdomain name.

9. Set up user attributes

Home > Enterprise applications | All applications > esterox

esterox | 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 Custom security attributes Security Activity Troubleshooting + Support

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

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 esterox.

- 1 Basic SAML Configuration

Identifier (Entity ID)	https://2leap.com/sso/simplesamlphp/www/module.php/saml/metadata.php?instance
Reply URL (Assertion Consumer Service URL)	https://2leap.com/sso/simplesamlphp/www/module.php/saml/sp/saml2-acs.php?esterox
Sign on URL	https://2leap.com/sso/index.php?sam1_sso=esterox
Relay State (Optional)	https://2leap.com/sso/index.php?sam1_sso=esterox
Logout URL (Optional)	Optional
- 2 Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
email	user.mail
subdomain	"esterox"
Unique User Identifier	user.userprincipalname
- 3 SAML Certificates

Token signing certificate	Active
Status	Active
Thumbprint	A6851F09A58882241F0933A65885A0BB39AE1650
Expiration	5/15/2027, 11:51:58 AM
Notification Email	telanias@telaniamail.com
App Federation Metadata URL	https://login.microsoftonline.com/v50962fe-adf1-...
Certificate (Base64)	Download
Certificate (Base6)	Download
Federation Metadata XML	Download

Microsoft Azure Search resources, services, and docs (G+7)

Home > Enterprise applications > eLeap-Azure-SSO > SAML-based Sign-on >

Attributes & Claims

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [named-for-...]

Additional claims

Claim name	Value
email	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname
subdomain	"trainingprovider"

Email and subdomain are mandatory, use your COMPANYSUBDOMAIN.

>> To add email and subdomain claims, click [Add New Claim]

Microsoft Azure Search resources, services, and docs (G+7)

Home > Enterprise applications > eLeap-APM SSO > SAML-based Sign-on >

Attributes & Claims

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [named-for-...]

Additional claims

Claim name	Value
email	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname
subdomain	"tecream"

Then enter [email] into the 'Name' field and select [user.mail] in the 'Source attribute' field:

Microsoft Azure Search resources, services, and docs (G+7)

Home > Enterprise applications > eLeap-APM SSO > SAML-based Sign-on > Attributes & Claims >

Manage claim

Save Discard changes Got feedback?

Name * email

Namespace Enter a namespace URI

Source * Attribute Transformation

Source attribute * user.mail

Claim conditions

To add [subdomain] attribute, click [Add new claim] and enter [subdomain] in the 'Name' field and your subdomain for example in our example 'icecream' in the 'Source attribute' field:

Microsoft Azure

Home > Enterprise applications > eLeaP APM SSO > SAML-based Sign-on > Attributes & Claims

Manage claim

Save Discard changes Got feedback?

Name * subdomain ✓

Namespace Enter a namespace URI ✓

Source * Attribute Transformation

Source attribute * "icecream" ✓

Claim conditions

Make sure to

click [Save]

10. Save the app

11. Send your metadata xml file to support@eleapsoftware.com

12. Go to app > properties and add a logo icon:

Microsoft Azure

Home > Enterprise applications > eLeaP APM SSO

eLeaP APM SSO | Properties

Overview Deployment Plan Manage Properties Owners Roles and administrators Users and groups Single sign-on Provisioning Application proxy Self-service Custom security attributes (preview) Security Conditional Access Permissions Token encryption Activity Sign-in logs Usage & insights Audit logs Provisioning logs

Save Discard Delete Got feedback?

View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. [Learn more.](#)

Enabled for users to sign-in? Yes No

Name * eLeaP APM SSO ✓

Homepage URL Enter a homepage URL

Logo Select a file

User access URL https://myapps.microsoft.com/signin/ca12b4d7-e2ce-45e0-a31b-99c2... ✓

Application ID ca12b4d7-e2ce-45e0-a31b-99c238ca16ea ✓

Object ID 2909610d-e911-496b-872f-687402c504e ✓

Terms of Service URI Publisher did not provide this information ✓

Privacy Statement URI Publisher did not provide this information ✓

Reply URL https://Zeap.com/sso/simplesamlphp/www/module.php/saml/sp/saml... ✓

Assignment required? Yes No

Visible to users? Yes No

Notes

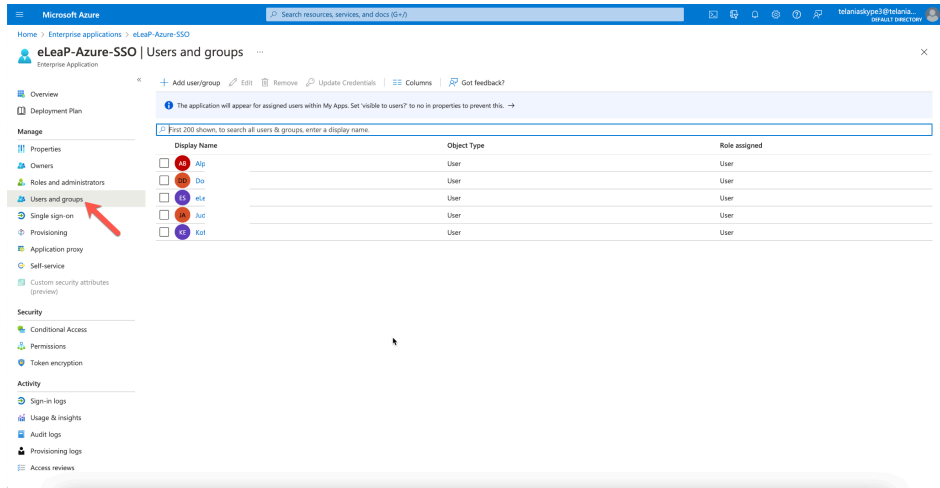
a.

https://www.eleapsoftware.com/wp-content/uploads/2020/01/eLeaP_logo_black.png

b.

https://www.eleapsoftware.com/wp-content/uploads/2020/01/eLeaP_logo_white.png

13. After eLeaP adds your metadata xml, you are ready to assign users to the app



Note: *Users must exist in eLeaP as well. You can use the bulk adding feature or the API to set up the users in eLeaP.*

Our Example Setup:

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 esterox.

1

Basic SAML Configuration

Edit

Identifier (Entity ID)	https://2leap.com/sso/simplesamlphp/www/module.php/saml/sp/metadata.php/esterox
Reply URL (Assertion Consumer Service URL)	https://2leap.com/sso/simplesamlphp/www/module.php/saml/sp/saml2-acis.php/esterox
Sign on URL	https://2leap.com/sso/index.php?saml_sso=esterox
Relay State (Optional)	https://2leap.com/sso/index.php?saml_sso=esterox
Logout Url (Optional)	Optional

2

Attributes & Claims

Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
email	user.mail
subdomain	"esterox"
Unique User Identifier	user.userprincipalname

3

SAML Certificates

Edit

Token signing certificate

StatusActive

ThumbprintAE851FD9A5B8B2241FD933A65B8B5A0BB39AE1650

Expiration5/15/2027, 11:51:58 AM

Notification Emailtelaniaskype3@telaniamail.com

App Federation Metadata Urlhttps://login.microsoftonline.com/a50962fe-adf1-...

Certificate (Base64)Download

Certificate (Raw)Download

Federation Metadata XMLDownload

Verification certificates (optional)

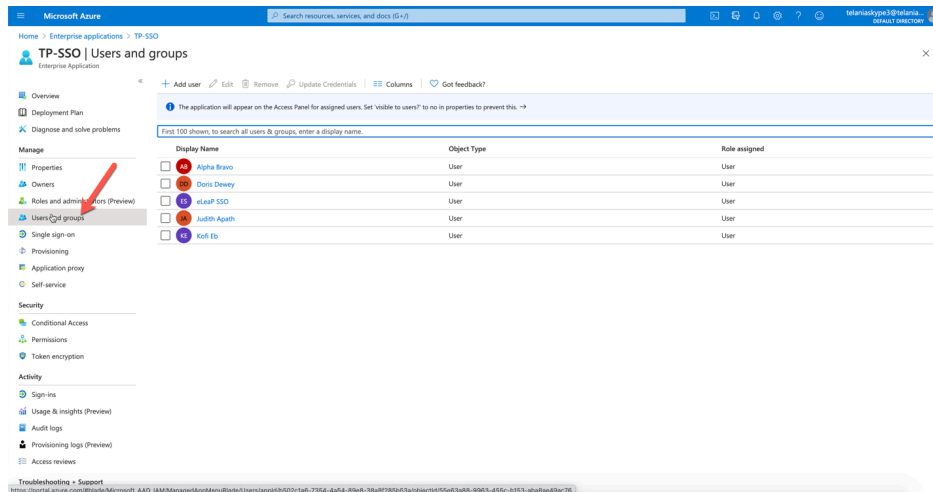
RequiredNo

Active0

Expiredn

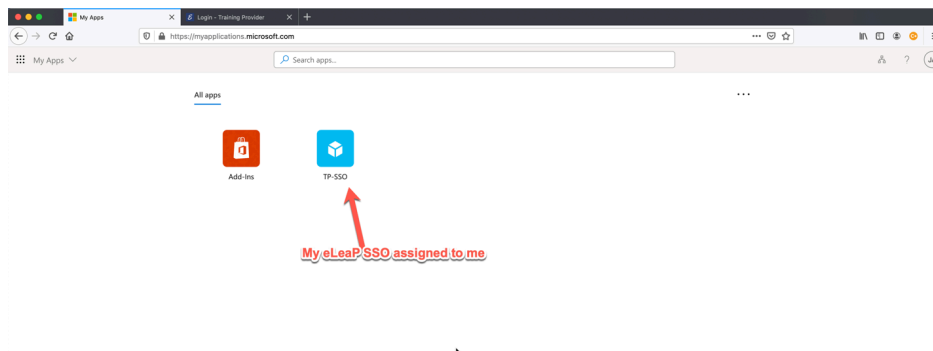
Edit

Once set up and the backend xml added, please assign users to the application:



User Login:

Microsoft has the <https://myapplications.microsoft.com/> URL for users to go in to access SSO and other applications. Users who are assigned to apps will see something like this:



FYI: Important

We noticed that in some cases, the AD user does not have their email field filled in. We manually added it to the user profile. This field is required for our SSO to work.

If you make any configuration changes, please download and send us the new xml file to add.

Microsoft Azure

Search resources, services, and docs (Ctrl-F)

tlantaskys3@telam...
DEFAULT DIRECTORY

Home > Enterprise applications > TP-SSO > Judith Apath

tlantaskys3@telam...
DEFAULT DIRECTORY

Judith Apath | Profile

User

✕

✕ Diagnose and solve problems

✕

Aug 23Aug 30Sep 6Sep 13Sep 20

Manage

Profile

Assigned roles

Administrative units

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

Activity

Sign-ins

Audit logs

Troubleshooting + Support

New support request

Identity

Name

Judith Apath

First name

Judith

Last name

Apath

User Principal Name

apath@telamtaskys3@telaminternal.onmicrosoft.com

User type

Member

Object ID

62626a46-9a1b-4996-b3bc-c1f6a3a7611e

Source

Azure Active Directory

Job info

Job title

Department

Manager

Company name

Employee ID

Settings

Block sign in

No

Usage location

Contact info

Street address

State or province

Country or region

Office

City

ZIP or postal code

Office phone

Mobile phone

Email

apath@telaminternal.com

Alternate email

Proxy address

View more

apath@telamtaskys3@telaminternal.onmicrosoft.com

Authentication contact info

Use the [Authentication methods](#) page to manage authentication contact info for a user