Tutorials

Tutorials in performing certain configurations

- Rancher-SAML-ADFS (Authentik)
- Organizr LDAP Setup (Authentik)
- LDAP Provider Generic Setup (Authentik)
- Steps to configure SAML 2.0 SSO with Microsoft Active Directory Federation Services
- iSpring Learn SSO with Azure AD + SAML
- Setting-up Azure Entra with Classlink
- Classlink LTI v1.3 (OIDC) Details
- Disable MFA in EntraID (Azure AD)

Rancher-SAML-ADFS (Authentik)

What is Rancher

> *An enterprise platform for managing Kubernetes Everywhere Rancher is a platform built to address the needs of the DevOps teams deploying applications with Kubernetes, and the IT staff responsible for delivering an enterprise-critical service.*
>
> *-- https://rancher.com/products/rancher*

Preparation

The following placeholders will be used:

- `rancher.company` is the FQDN of the Rancher install.
- `authentik.company` is the FQDN of the authentik install.

Under *Customization -> Property Mappings*, *create a SAML Property Mapping*. Give it a name like "SAML Rancher User ID". Set the SAML name to `rancherUidUsername` and the expression to the following

```
return f"{user.pk}-{user.username}"
```

Create an application in authentik. Set the Launch URL to `https://rancher.company`, as Rancher does not currently support IdP-initiated logins.

Create a SAML provider with the following parameters:

- ACS URL: `https://rancher.company/v1-saml/adfs/saml/acs`
- Audience: `https://rancher.company/v1-saml/adfs/saml/metadata`

- Issuer: `authentik`
- Service Provider Binding: `Post`
- Property mappings: Select all default mappings and the mapping you've created above.
- Signing Certificate: Select the authentik self-signed certificate.

You can of course use a custom signing certificate, and adjust durations.

Rancher

In Rancher, navigate to *Global -> Security -> Authentication*, and select ADFS.

Fill in the fields

- Display Name Field: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`
- User Name Field: `http://schemas.goauthentik.io/2021/02/saml/username`
- UID Field: `rancherUidUsername`
- Groups Field: `http://schemas.xmlsoap.org/claims/Group`

For the private key and certificate, you can either generate a new pair (in authentik, navigate to *Identity & Cryptography -> Certificates* and select Generate), or use an existing pair.

Copy the metadata from authentik, and paste it in the metadata field.

Click on save to test the authentication.

rancher-f02ae6fd4286551b6a052d80fabbaa61.png

Organizr LDAP Setup (Authentik)

Support level: Community

What is organizr

> *Organizr allows you to setup "Tabs" that will be loaded all in one webpage.*
>
> *-- https://github.com/causefx/Organizr*

This integration leverages authentik's LDAP for the identity provider to achieve an SSO experience. See ldap provider generic setup for setting up the LDAP provider.

Preparation

The following placeholders will be used:

- `organizr.company` is the FQDN of the Service install.
- `authentik.company` is the FQDN of the authentik install.

Create a new user account *(or reuse an existing)* for organizr to use for LDAP bind under *Directory* -> *Users* -> *Create*, in this example called `ldapservice`.

Note the DN of this user will be `cn=ldapservice,ou=users,dc=ldap,dc=goauthentik,dc=io`

> *Optionally*, create a new group like `organizr users` to scope access to the organizr application.

Authentik Configuration

1. Create a new Proxy Provider for `https://organizr.company`
organizr1-b1ef217babbce02ddddc22a8c32ebda6.png *Optionally*, add the regular expression to allow api calls in the advanced protocol settings. organizr2-d280f1ddb23fa548df44ed29c4bc1d39.png
2. Create a new Application for the `https://organizr.company` Provider.
organizr3-9421eebe818e0fd54c3b0f66f8ebaed3.png

> TIP
> *Optionally*, bind the group to control access to the organizr to the application.

3. organizr4-3a2635f55a9df6ce3e587af7fd6c218e.png

organizr5-b8a1743daff42f30b84ab3b051e916d9.png ::: 3. Add the Application to the authentik Embedded Outpost.

organizr Configuration

> CAUTION
> Ensure any local usernames/email addresses in organizr do not conflict with usernames/email addresses in authentik.

1. Enable Auth Proxy in organizr *system settings -> main -> Auth Proxy*

Auth Proxy Header Name: `X-authentik-username` Auth Proxy Whitelist: *your network subnet in CIDR notation IE* `10.0.0.0/8` Auth Proxy Header Name for Email: `X-authentik-email` Logout URL: `/outpost.goauthentik.io/sign_out` organizr6-a4fb29e0896bfe7f64c88cb1c9546c22.png

2. Setup Authentication in organizr *system settings -> main -> Authentication*

Authentication Type: `Organizr DB + Backend` Authentication Backend: `Ldap` Host Address: `<LDAP Outpost IP address:port>` Host Base DN: `dc=ldap,dc=goauthentik,dc=io` Account Prefix: `cn=` Account Suffix: `,ou=users,dc=ldap,dc=goauthentik,dc=io` Bind Username: `cn=ldapservice,ou=users,dc=ldap,dc=goauthentik,dc=io` Bind Password: `<LDAP bind account password>` LDAP Backend Type: `OpenLDAP` organizr7-a95d978bd21069853ff57f4510e5e982.png

> INFO
> Access for authentik users is managed locally within organizr under *User Management*. By default, new users are assigned the `User` group.

TIP

Consider front-ending your application with a forward auth provider for an SSO experience.

LDAP Provider Generic Setup (Authentik)

Create User/Group

1. Create a new user account to bind with under *Directory -> Users -> Create*, in this example called `ldapservice`.
   Note the DN of this user will be `cn=ldapservice,ou=users,dc=ldap,dc=goauthentik,dc=io`
2. Create a new group for LDAP searches. In this example `ldapsearch`. Add the `ldapservice` user to this new group.NFO

> Note: The `default-authentication-flow` validates MFA by default, and currently everything but SMS-based devices are supported by LDAP. If you plan to use only dedicated service accounts to bind to LDAP, or don't use SMS-based authenticators, then you can use the default flow and skip the extra steps below and continue at Create LDAP Provider

LDAP Flow

Create Custom Stages

1. Create a new identification stage. *Flows & Stage -> Stages -> Create*
   general_setup1-28b081e6970d26d4c2bf089c6db0c572.png
2. Name it something meaningful like `ldap-identification-stage`. Select User fields Username and Email (and UPN if it is relevant to your setup).
   general_setup2-aedc0968da698af2d004996d6bf32172.png
3. Create a new password stage. *Flows & Stage -> Stages -> Create*
   general_setup3-23a6d9635092816513b8bedcf5827ddb.png
4. Name it something meaningful like `ldap-authentication-password`. Leave the defaults for Backends.
   general_setup4-9f6514bc905e1c7fa252313c83b443e6.png
5. Create a new user login stage. *Flows & Stage -> Stages -> Create*
   general_setup5-b9e688db2f3f23b57cdd23ab3ce74182.png
6. Name it something meaningful like `ldap-authentication-login`.
   general_setup6-a39cb7f17b1e677695ad7ac20659fc36.png

Create Custom Flow

1. Create a new authentication flow under *Flows & Stage -> Flows -> Create*, and name it something meaningful like `ldap-authentication-flow`
general_setup7-5d28d5df6b1b2e69952919bfe30779b5.png
2. Click the newly created flow and choose *Stage Bindings*.
general_setup8-514c7914c49400ee061d0a0df8e2b9f5.png
3. Click `Bind Stage` choose `ldap-identification-stage` and set the order to `10`.
general_setup9-6a04b5c7c774b548fdd3dcdb887a155f.png
4. Click `Bind Stage` choose `ldap-authentication-login` and set the order to `30`.
general_setup11-efd91bc25673f7df384b6d60de33f085.png
5. Edit the `ldap-identification-stage`. general_setup12-25cc9fcea6654935c3587b21922b77fd.png
6. Change the Password stage to `ldap-authentication-password`.
general_setup13-a5006f341fdab49f32894d50e769a9c7.png

Create LDAP Provider

1. Create the LDAP Provider under *Applications -> Providers -> Create*.
general_setup14-9c2a270903b5bf88b693884c22d32c96.png
2. Name is something meaningful like `LDAP`, bind the custom flow created previously (or the default flow, depending on setup) and specify the search group created earlier.
general_setup15-3935cd6f3c497e436edacb53bec095e1.png

Create LDAP Application

1. Create the LDAP Application under *Applications -> Applications -> Create* and name it something meaningful like `LDAP`. Choose the provider created in the previous step.
general_setup16-1c57654a5ad05b12d3a21fd58e0e8350.png

Create LDAP Outpost

1. Create (or update) the LDAP Outpost under *Applications -> Outposts -> Create*. Set the Type to `LDAP` and choose the `LDAP` application created in the previous step.
general_setup17-1a8524a769f4f4d24e59522be62ea6cb.png

> INFO
>
> The LDAP Outpost selects different providers based on their Base DN. Adding multiple providers with the same Base DN will result in inconsistent access

ldapsearch Test

Test connectivity by using ldapsearch.

INFO

ldapsearch can be installed on Linux system with these commands

```
sudo apt-get install ldap-utils -y # Debian-based systems
sudo yum install openldap-clients -y # CentOS-based systems
```

```
ldapsearch \
  -x \
  -h <LDAP Outpost IP address> \
  -p 389 \ # Production should use SSL 636
  -D 'cn=ldapservice,ou=users,DC=ldap,DC=goauthentik,DC=io' \
  -w '<ldapuserpassword>' \
  -b 'DC=ldap,DC=goauthentik,DC=io' \
  '(objectClass=user)'
```

INFO This query will log the first successful attempt in an event in the *Events -> Logs* area, further successful logins from the same user are not logged as they are cached in the outpost.

Manual Outpost deployment in docker-compose

To deploy an outpost with docker-compose, use this snippet in your docker-compose file.

You can also run the outpost in a separate docker-compose project, you just have to ensure that the outpost container can reach your application container.

Proxy outpost

```
version: "3.5"

services:
```

```
    authentik_proxy:
        image: ghcr.io/goauthentik/proxy
        # Optionally specify which networks the container should be
        # might be needed to reach the core authentik server
        # networks:
        #   - foo
        ports:
            - 9000:9000
            - 9443:9443
        environment:
            AUTHENTIK_HOST: https://your-authentik.tld
            AUTHENTIK_INSECURE: "false"
            AUTHENTIK_TOKEN: token-generated-by-authentik
            # Starting with 2021.9, you can optionally set this too
            # when authentik_host for internal communication doesn't match
the public URL
            # AUTHENTIK_HOST_BROWSER: https://external-domain.tld
```

LDAP outpost

```
version: "3.5"

services:
    authentik_ldap:
        image: ghcr.io/goauthentik/ldap
        # Optionally specify which networks the container should be
        # might be needed to reach the core authentik server
        # networks:
        #   - foo
        ports:
            - 389:3389
            - 636:6636
        environment:
            AUTHENTIK_HOST: https://your-authentik.tld
            AUTHENTIK_INSECURE: "false"
            AUTHENTIK_TOKEN: token-generated-by-authentik
```

Steps to configure SAML 2.0 SSO with Microsoft Active Directory Federation Services

PRODUCTS: Learn

Note: ADFS 2.0 on Windows Server 2008 r2 or ADFS 3.0 on Windows Server 2012 / 2012 r2)

SAML 2.0 single sign-on (SSO) supports integration with Microsoft Active Directory Federation Services (ADFS) 3.0.

Requirements

- A fully installed and configured ADFS service.
- A server running Microsoft Server 2008r2 or 2012/2012r2
- An SSL certificate to sign your ADFS login page and the thumbprint of that certificate

In this example we are using ADFS 2.0 on Windows Server 2008 R2. On Windows Server 2012 the steps will be the same except for the installation, because you install AD FS role via the server manager, not via the installation package as on Windows 2008 server r2.

Step 1. AD FS Management

Login in to your AD FS server and launch the ADFS Management Console via the shortcut in Control Panel\Administrative Tools.

txyVmpwGv__tSTGJwXYyz0yC82ytijIjSb4t7TwX5aj2V7PBfMQHxioflnVrcd2zqsxe_DCaLQ3rsJMBsv1erQR9aFIR

Step 2. Check AD FS settings

Right-click on Service and sel ect Edit Federation Service Properties...

vpNhOmi5zA7XXr4zymN9Z2U4N5FQ5qsIaRdfJlknxBk8uXBO9wYo_mC3WsG9XQTJb6O4Z7eMNRwPlr_51L8tJ

Confirm that the General settings match your DNS entries and certificate names. Make a note with the Federation Service Identifier, since that is used in the iSpring Learn SAML 2.0 configuration settings.

1sY5XuJ0_hrWRWv07Qgv4f6mznJNfcQAYm-QLkN49QtLoExMMAmvhoD3SdVgo9KN9DjG92zjt3vjiWaKVjZxH3p

Step 3. Token-Signing certificate

1. Browse to the certificates.
2. Right-click on the certificate and sel ect View Certificate.
3. Go to the Details tab.
4. Find the Thumbprint field and copy the contents of this field to the Windows clipboard.

RWYwuaq5guXjKsQRWl50CwbHAbzlSJh2QVh-T9xA5xKBVihAiVxMs3YCTJ_xcGv7XzqWnqLGXOkponiAJjjcXb_

Step 4. Learn Settings

1. Log in into your iSpring Learn account and go to the SSO settings via this link: https://YourAcc?untURL.ispringlearn.com/settings/sso
2. Ins ert your Thumbprint into the Certificate Fingerprint field and remove all spaces between characters.
3. Enter your data to the Metadata URL, Sign ON URL and Logout URL fields.

SAML01.png

Step 5. ADFS Relying Party Configuration

Go to the ADFS Management console and select Relying Party Trusts, right-click on it and select Add Relying Party Trust…

DWe2TCjpUD-9mwb9YE-Yi_3VQvvLo6w5S4K9Tqo5iu3ytTrfMkakrv2THOkYo9HFrYZJMUyGxQCOOha-7EbJ_m

Select Next On the Welcome Screen of the wizard, and on the Select Data Source step, select the last option: Enter data about the relying party manually.

FedR8yJMFy79Wm7ZOapfx8-RgWO8Syz-VFPk5VezbDvw_urdX2UCWCFEakA7sMeQsRcVARsoJKANp8gKd0V

On the next screen, enter a Display name that you will recognize in the future.

gHTy1NaSaFcC9tAVCwq4nrI2YFD9YJQ8j_BVccexWw2E6wWMG9kkBI4su3Mf_kGmhhPf5lkCm-8p5W6i-L6119h

Next, select AD FS profile:

phGZye3RG4RuFv7kujBnkKtD75sg-YOU4hPlQHv--3weu7qnzB2QgwYSJ5a0vEWititNIzz_WbNDbojReboku0G12

Leave the default values:

E2twaBJWzoKspzzxkn-26XSsvalo8wAL3ayJYM3fVtszGyegf2o4-729bwV7jzammYv6Az1Ew2Mj--G3Kw4NZo0Ok

On the next screen, check the box labeled: Enable support for the SAML 2.0 WebSSO protocol. The service URL will be: https://YourAcc?untURL.ispringlearn.com/module.php/saml/sp/saml2-acs.php/default-sp

eJxJWt1KAQ5E7ldDZmtzrdiFB4icMGUHoVL5pDbAwO98o8CgHPIBOF73CHPQ6H1Cm7HuPbN4z-ZLf3Qt_ygNT

Click Next. Add Relying party trust identifier: https://YourAcc?untURL.ispringlearn.com/module.php/saml/sp/metadata.php/default-sp

X1S7UllJ3QhuitOZkPPDzm9GvR_oh0MZafS1VP4cMpGRNfmg8TVDzDePguMRDbQ61VwLaHMK6B2UuYIX_s4

Choose Permit all users to access this relying party.

_Dgqb5gnSjLRvtQKuIQ38K9wkVb97WYKFZXIiQb6OFAzlChmaFRNlH5H3J-YNS5h8j8it6BHfHADt88WfhCoUS3k

On the next step, just click Next.

AX0Y9Y9a0Al-EQAgUkmNTSC-tTxJXVe0K1G2fBf9_ZofD5PPBD9wltrEo1A6Av-SvpJwQ_bUibkawPZSjL-YMmJc

On the final screen, check the box Open the Edit Claim Rules dialog and use the Close button to exit.

ZS3_FXPmR5XFVIL4PE_wc5XczVkdUAtV17oG6Ed3qghwAdibKNFwmA8pISzu0ZUDoEvST2PA4NDgK_wLCb_

Step 6. Creating Claims Rules

1. Add the first rule
   ZUjVMXbGp0OoUkrJbpP90Tbgdx0vhmO6okP5lNz5kHXPxFqZ8zXCP22BK-mP0oYJKT3e0q4T1Al7pVMXfV
2. Select Send LDAP Attributes as Claims
   PfGJ2OSpACIm1nBtinVxH-hRr2IX7JsiG8V0wOASvZzD_5ohgTa5uQk3jFRwr9V8KcsIBSwBpNGBniGTAZpp
3. On the next screen, specify your Claim Rule, for Example E-mail to Learn, using Active Directory as your attribute store, and do the following:

1. Fr om the LDAP Attribute column, select E-Mail Addresses
2. Fr om the Outgoing Claim Type, enter “email” cbshGH1pmCu-u_um9H9JSU9MicGTn1jaoESRcZbqGhYy_wDAWT5TLi-7xjBvnhtoZx7NVxYAiKfRP75JD
3. Click on Finish or OK to save the new rule

4. After that, add the second rule and select Transform an Incoming Claim as the template Vldhqs282322jhhTUzugw7MZQzkKPrypE-UkoNmWx-D0X3cnlLQS2M6KVa82ORZ8ZFkPR9MjRRSmOUplU
   1. Give your Claim Rule a title, for example, Transform Account Name
   2. Select Windows account name as the Incoming Claim Type
   3. Under Outgoing Claim Type, select Name ID
   4. Under Outgoing Name ID Format, select Transient Identifier
   5. Leave the default rule Pass through all claim values J22FEWcG11f_f7Wta7PB0GepLEwafkUvUNuori6HE5SqEZqqiNS0HuTJ56PUaV-WiSsyUVHVAPops4QY
5. Finally, click on OK to create the claim rule, and then OK again to finish creating rules.

Step 7. Adjusting the Trust Settings

Some settings on your Relying Party Trust will need to be adjusted. To access these settings, select Properties from the Actions sidebar on the right while you have the Relying Party Trust selected.

- Under the Advanced tab, make sure that the selection is SHA-1 gNd4s8hFJrd4hzspladUgmtg60Q9bna6nn0O0q5TpNfkdwMr0dCftiWCFgT1mMPwQOg4BNuWQ8cMWYooU
- Under the Endpoints tab, click ADD to add a new endpoint
- For the Endpoint type, select SAML Assertion Consumer
- For the Binding, choose Artifact with Index 2
- The URL field should look like this: https://YourAcc?untURL.ispringlearn.com/module.php/saml/sp/saml2-acs.php/default-sp
- Leave the Response URL blank and click on OK gsGicTEDLYbI9F0K7iJIIWm_jmnD4rYS8dQeJDEM3ncvix3uMW4v1mWmEb5FKKkC3JKwNAFs9HfLpYDHU
- Click ADD one more time
- For the Endpoint type, sele ct SAML Logout
- For the Binding, choose POST

- The URL field should look like this: https://Y?UR_ADFS_SERVERNAME.domail.local/adfs/ls/?wa=wsignout1.0
- Leave the Response URL blank and click on OK
gf1gpP3TETi2aIqvn79UxX2UY5Y8lxXS6bneJEpQMkBBKEAOq998XfDnZXm6Kd4FNgCBWknm-wEm1BAe6

Step 8. Logging

Go to your SSO login page: https://YourAcc?untURL.ispringlearn.com/sso/login and enter your credentials.

Related Articles

- Integrating iSpring Learn with your system: User Management and Single Sign On
- SAML Technology for SSO
- iSpring Learn SSO with Azure AD + SAML

iSpring Learn SSO with Azure AD + SAML

PRODUCTS: Learn

Azure Active Directory (Azure AD) is a part of the Microsoft Azure cloud service that makes it possible to enjoy SSO (Single sign-on) without employing on-prem AD FS (Active Directory Federated Services). It is basically a cloud alternative to Microsoft Active Directory. In this scenario, there is no need to maintain an on-premise infrastructure, the process of setting it up is rather easy, and it works with most cloud-based services.

Requirements

A Microsoft Azure account with Azure AD Premium activated.

How to set up Azure AD

1. Go to the Microsoft Azure Home Page. From the Azure services menu, select Enterprise applications.
   01.png
2. Select New application.
   02.png
3. Select **Create your own application**.
   03.png
   In the right-side menu that appears, enter the name for the application, such as iSpring Learn SSO.
   04.png
4. Click Create and wait until the application is added to your library. You will then be redirected to the Overview page.

   In the sidebar menu, select Users and groups. There, you can add all the users who should be able to log into their iSpring Learn account using SSO.
   05.png
5. In the sidebar menu, select **Single sign-on**. Then, select **SAML for SAML-based SSO**.
   06.png

Set up Single Sign-On with SAML. Here’s how:

First, select Edit, to open the right-side menu.
07.png

In the right-side menu, fill out Identifier (Entity ID), Reply URL, and Relay state as shown in the table below, where ‘_____’ is the first part of the URL of your iSpring Learn account. Pay attention to the domain for your iSpring Learn account: it is either .com or .eu.

Identifier (Entity ID)	https://_____.ispringlearn.com/module.php/saml/sp/metadata.php/default-sp
Reply URL	https://_____.ispringlearn.com/module.php/saml/sp/saml2-acs.php/default-sp
Relay state	https://_____.ispringlearn.com/sso/login

08.png

Save the changes.

1. Second, select

Edit

1. to edit User Attributes and Claims.

09.png

The first claim in the list is the Required claim. Its claim name is Unique User Identifier (Name ID) and its Value is user.mail. It is there by default. Leave it as it is.

The additional claims are those used by iSpring Learn to sync the data about your users and fill out their user profiles in iSpring Learn. The information will be updated in iSpring Learn each time you log in.

1. Since iSpring Learn requires each user to have a login, this is the required claim. We also strongly recommend using email so your users get notifications from the system about new courses assigned, coming deadlines, and scheduled meetings and webinars. The rest of the claims are optional.

1. Delete the preset claim names and values and add your own. You can use your own names for the claims while you select values from the available list. To simplify the process, we recommend using the same claim name as the value. The only exception is user.login, where we use user.mail, thus making the login correspond with the email. Use the table below for the correct claim names and their values.

Claim Name	Value
user.login	user.mail
user.mail	user.mail
user.surname	user.surname
user.givenname	user.givenname
user.jobtitle	user.jobtitle

1. Only the Name and the Source Attribute fields need to be changed. Leave the rest empty.

11.png

1. When you are done, you should see the list of all the claims you want your iSpring Learn account to be in sync with.

10.png

Note that you won't be able to sync the user's country and department.

1. Return to the previous page to configure the third step: the certificate. Select **Add a certificate** to open the menu on the right side of the screen and select **New Certificate**.
   12.pngFor **Signing Option**, select **Sign SAML assertion**. For **Signing Algorithm**, select **SHA-1**. Select **Save** for the certificate to be generated and the thumbprint to be displayed. You will need the thumbprint when you configure the connection settings in iSpring Learn.

   Close the menu on the right side of the screen to return to configuring the fourth step: iSpring Learn SSO.

   The data from this step should be used in the Connection Settings of your iSpring Learn account.

How to set up iSpring Learn

1. Log into your iSpring Learn account and go to https://_____.ispringlearn.com/settings/sso
2. In Connection Settings, fill in the fields with the information from Azure.

iSpring Learn name	Azure name
Issue URL (IdP Entity ID)	Azure AD Identifier

Sign-on URL	Login URL
Logout URL	Logout URL
Certificate Fingerprint	Thumbprint

13.png
If you have selected the **Redirect users to the SSO login page**, the user will be automatically redirected to the Azure login page when they open iSpring Learn. If they are already logged in there, they will see their main page with the courses that have been assigned.

If this option is not selected, upon opening iSpring Learn, the user will see the default login screen with an additional option to use a corporate account to log into the account.

We recommend keeping this option deselected initially for the sake of testing the connection and to avoid being locked out of your iSpring Learn account. If this happens for some reason, you can use https://____.ispringlearn.com/login?no_sso to bypass SSO.

Proceed to Matching fields of iSpring Learn with the external SSO attributes and use the claims you created in the second step of the Azure Set up Single Sign-On with SAML page.
14.png

When done, scroll up and click **Save**.

You can now test the connection.
15.png

If something is not clear or additional questions arise, don't hesitate to contact us at support@ispring.com and we'll do our best to assist you.

Related Articles

- SAML Technology for SSO
- Integrating iSpring Learn with your system: User Management and Single Sign On
- How to upload SCORM courses to ...

Setting-up Azure Entra with Classlink

Notes

This is an all or none type of configuration. Once enabled all users of the domain will be redirected to Launchpad for authentication in all Microsoft applications. Users previously Authenticated to Office 365/Entra ID (Azure AD) may need to reauthenticate their desktop applications. Office365 Administrator accounts will not be affected by this workflow.

Prerequisites

- Authenticate to LaunchPad with AD (technically could be Google as well but unlikely)
  - District's Azure user profile **must** contain an ImmutableI
  - If the district uses Azure AD Connect, it's handled
  - If the district enters users manually, it's handled
  - If the district uses OneSync for Azure, it can be handled in the configuration
- Add Verified Domain to Entra ID (Azure AD)
  - Do not make it primary.
- Install MSOnline PowerShell module

```
Install-Module MSOnline
```

- Install Azure Active Directory Connect and configure it – Do not federate via this method.
- Active Directory should be connected in launchpad under settings > domain gear icon
- Active Directory Groups should be imported into launchpad

Step 1

1. In the Classlink tenant SAML Console, Create a new SAML configuration by copying existing and selecting "A New SAML App (template)"
2. Configure the following options.

- Metadata URL
  - https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationme tadata.xml
- Loginurl with custom login, e.g. https://launchpad.classlink.com/<customurl>
- Attribute Mapping

- ? Select “Custom Attribute”
  - Change name of the custom attribute to “IDPEmail”
  - Add {email} in the data field

- MetaOverrides
  - Logout Service URL (POST)
    - https://login.microsoftonline.com/common/oauth2/logout

  - NamedID Format
    - Persistent

  - NameID Custom Value
    - {ldapguid:hexbase64}

- Save or Update

Step 2

- Copy the metadata URL and modify the PowerShell Script below
- Use this PowerShell Script, change the file extension to “.ps1” after downloading - You may need to unblock the file and change your execution policy on the server
  - Google Drive

Azure AD PowerShell Code

```
<#
.SYNOPSIS
    Federate Microsoft Entra ID (Azure AD/Microsoft Online Services) to
ClassLink for IdP Services.

    Change the <GUID> in the $idpMetadataUrl to be the GUID from your
SAML console App.
    Change $DomainName to match your domain name that is going to be
Federated
    Change the script extension to ".ps1"

    *NOTE: you may need to set the PowerShell Execution Policy to remote
signed or bypass temporarily.

#>
```

```
Install-Module -Name MSOnline
Import-Module MSOnline

$idpMetadataUrl = "https://idp.classlink.com/sso/metadata/<GUID>"

$DomainName = "<your domain name>"
$metadataxml = [Xml](Invoke-WebRequest -Uri $idpMetadataUrl -ContentType
"application/xml").content

$cert = -join
$metadataxml.EntityDescriptor.IDPSSODescriptor.KeyDescriptor.KeyInfo.X509
Data.X509Certificate.Split()
$issuerUri = $metadataxml.EntityDescriptor.entityID
$logOnUri =
$metadataxml.EntityDescriptor.IDPSSODescriptor.SingleSignOnService | ? {
$_.Binding.Contains('Redirect') } | % { $_.Location }
$LogOffUri =
$metadataxml.EntityDescriptor.IDPSSODescriptor.SingleLogoutService | ? {
$_.Binding.Contains('Redirect') } | % { $_.Location }
$brand = "ClassLink Identity"
Connect-MsolService
$DomainAuthParams = @{
    DomainName = $DomainName
    Authentication = "Federated"
    IssuerUri = $issuerUri
    FederationBrandName = $brand
    ActiveLogOnUri = $logOnUri
    PassiveLogOnUri = $logOnUri
    LogOffUri = $LogOffUri
    SigningCertificate = $cert
    PreferredAuthenticationProtocol = "SAMLP"
}

Set-MsolDomainAuthentication @DomainAuthParams
```

If you receive an error regarding scripts being disabled Open an elevated PowerShell prompt Type the following:

```
set-executionpolicy remotesigned -force
```

This will allow local PowerShell scripts to run

? If you use an account that is being federated (using the custom domain instead of an onmicrosoft.com domain) https://portal.azure.com should redirect you to https://launchpad.classlink.com/<customurl> for login from now on, along with any other Microsoft Service

Step 3:

- Make sure you have break-glass accounts within Microsoft in case something happens.
  - https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-acc ess

Revert to Entra ID (Azure AD) Managed Authentication

Open PowerShell

1. Run the command
2. Connect-MsolService

After authenticating to your Entra ID (Azure AD) Tenant

Run the command:

```
  Set-MsolDomainAuthentication -authentication managed -domainName
<domainname>
```

> Replace `<domainname>` with your domain you wish to remove federation

Classlink LTI v1.3 (OIDC) Details

Dear Vendor,

Our school is going to add your app as an LTI v1.3 SSO app through ClassLink. Please provide me with the following information:

- ClientID (generated in the Partner Portal)
- OIDC Login Initiation URL
- Target Link URL
- LTI Message Type (default is LtiResourceLinkRequest)
- Person SourcedID
- Role
- With PII
- Any Input Fields that I would need

Here is information about our school system and ClassLink:

- The OpenID Connect (OIDC) discovery endpoint is https://launchpad.classlink.com/.well-known/openid-configuration
- The OIDC discovery endpoint contains the following:
    - Issuer ID: https://launchpad.classlink.com
    - OIDC URL: https://launchpad.classlink/com/oauth2/v2/auth
    - JWKS URL: https://launchpad.classlink/com/oauth2/v2/jwks
- Our SchoolDeployment ID (Tenant ID) is xxxx. (Not all vendors require a Deployment ID, but it's best to include it in case it is needed.)

Thank you so much for your help with this,

Insert Your Name and Contact Information

Disable MFA in EntraID (Azure AD)

1. You are using 3rd party MFA which is ClassLink, is this correct?

2. You want to disable the Microsoft MFA, or you do not wish your users to be asked for a Microsoft MFA, is this correct?

-If yes is your answer the above information, disable the following: "Registration Campaign", "System-Preferred Multi-factor Authentication" and your tenants "Security Defaults".

3. To disable the "Registration Campaign":

- Go to > https://portal.azure.com >Microsoft Entra ID >Manage >Security >Authentication Methods >Registration Campaign >switch the State from Enabled or Microsoft Managed to Disable.

4. To disable the "System-Preferred Multi-factor Authentication"

- Go to > https://portal.azure.com >Microsoft Entra ID >Manage >Security >Authentication Methods >Settings >System-Preferred Multi-factor Authentication >switch the State from Enabled or Microsoft Managed to Disable.

5. To disable the "Security Defaults"

- Go to > https://portal.azure.com??????? >Microsoft Entra ID >Manage >Properties >Manage Security Defaults >switch from Enable to Disable.