Install Skolon as an external Identity Provider (IDP) to Entra

Skolon Support - 2025-04-22 - Integrations

In this article, you'll learn the steps to configure Skolon as a SAML identity provider (IdP) for Entra. Once configured, users will be able to use their Skolon credentials or Skolon Pass (QR-codes) to sign in to Entra account, as well as inTune enrolled Windows 11 devices.

Please note that if your district would like to utilize Skolon pass (QR-codes) as authentication method to inTune enrolled Windows 11 devices, you will need to complete the steps listed in two articles - this article as well as (insert article).

Prerequisites
The configuration of Skolon Pass as an IdP for Entra relies federating one or multiple domains in Entra and placing the users in this domain. The domain federation is done Entra in turn relies on their attribute “Immutable ID” to map users signing in with an external IdP to their Entra account.

Once an existing user is moved to a federated domain with an external IdP they have to use the federated IdP to sign in. As a precaution to avoid impacting existing users, we recommend testing the entire SSO flow on a test domain and test user initially. This article includes steps to create a user in Entra for testing purposes.

To configure Skolon as an IdP for Entra ID, the following prerequisites must be met in **Entra**:

- An Entra ID tenant with atleast one verified domain available in the Entra Admin Center
    - Only root domains can be federated. If you have a subdomain, you must promote it to a root domain before federation. For more details about root domain and federation see Microsoft official documentation.
- Access to Entra ID with an account with the Global Administrator role
- All users have Entra ID account created.
    - We recommend using the Skolon Entra LCM integration for this purpose, however it’s not required that users are created through this integration
- All users have Immutable ID’s set in their Entra ID account
    - If your existing integrations for creating Entra accounts set Immutable ID’s, Skolons Entra Update Sync is required.
    - If you have no Immutable ID’s set in Entra, Skolons Immutable ID-sync is

required

To configure Skolon as an IdP for Entra ID, the following prerequisites must be met in **Skolon**:

- Access to the Skolon Platform and the Data Hub with the Organization admin role
- All users have a Skolon account created
- All users have their Immutable ID from Entra set in Skolon
    - For instructions on how to generate and/or set Immutable ID's with integrations from Skolon, read the following article
- Knowledge on how to generate Skolon Pass for users in Skolon

Federating a domain
Ensure you are running PowerShell as an administrator and that you have an Entra admin account before beginning the federation process. The PowerShell commands in steps 1, 2 and 3 are mandatory.

Step 1. Connect to your Microsoft Entra Directory as tenant administrator

Run the following script in PowerShell:

```
Connect-MgGraph -Scopes "Directory.AccessAsUser.All
Directory.Read.All Directory.ReadWrite.All Domain.Read.All
Domain.ReadWrite.All"
```

Step 2. Enter federation configuration

Run the following script in PowerShell - you will get all the variable information from your Skolon Representative.

```
$Domain = $Domain

$federationBrandName = "Skolon"

$ActiveSignInUri = $ActiveSignInUri

$PassiveSignInUri = $PassiveSignInUri

$IssuerUri = $IssuerUri

$Protocol = "saml"

$federatedIdpMfaBehavior = "acceptIfMfaDoneByFederatedIdp"
```

```
$SigningCertificate = $cert
```

$SigningCertificate - Get the signing certificate here: https://saml-idp.skolon.com/metadata-certificate/

Step 3. Configure your domain for federation with Skolon

Run the following script in PowerShell:

```
New-MgDomainFederationConfiguration -DomainId $Domain -
ActiveSignInUri $ActiveSignInUri -IssuerUri $IssuerUri -
PassiveSignInUri $PassiveSignInUri -PreferredAuthenticationProtocol
$Protocol -federatedIdpMfaBehavior $federatedIdpMfaBehavior -
SigningCertificate $SigningCertificate
```

Step 4. Ensure that the federation configuration is successfully created on your domain

Run the following script in PowerShell:

```
Get-MgDomainFederationConfiguration -DomainId $Domain
```

Step 5. Create test user in Entra

This step is required only if you want to test the end-to-end flow with a test user. A test user has to be created in Skolon with the same immutableId used when creating the test user in Entra.

You can update any fields while creating the test to your liking, but make sure the following attributes are set:

- UserPrincipalName - use the federated domain configured in step 2 for the user
- OnPremisesImmutableId - has to be identical to the immutableId set on the user account in Skolon.
- OtherMails

```
$Password =  "Web4Lov16JU/"

$PasswordProfile = @{

    Password = "$Password"

    ForceChangePasswordNextSignIn = $false

}
```

```
New-MgUser `

   -UserPrincipalName "johndoe@federated.domain" `

   -DisplayName "John Doe" `

   -GivenName "John" `

   -Surname "Doe" `

   -AccountEnabled `

   -MailNickName 'JohnDoe' `

   -OnPremisesImmutableId johndoe@federated.domain`

   -OtherMails "johndoe@federated.domain" `

   -PasswordProfile $PasswordProfile

//--------------------------------

$Password =  "SecurePass21XY"

$PasswordProfile = @{

    Password = "$Password"

    ForceChangePasswordNextSignIn = $false

}
```

Step 6. Create a test user in Skolon

Create a test user on any school in your Skolon environment. Make sure the immutableId used in Skolon is identical to the one used when creating the test user in step 5.

Instructions on how to create a user manually can be found in the article

If you want to test the SSO flow with Skolon Pass, make sure you generate and activate a QR-code for the user as described in the article

Test sign-in flow in the web

Once step 1-6 is completed you are ready to test the SSO flow in the web with the test user. Here's what the login process to test the flow on web will look like:

1. Open an incognito window in your browser.
2. Navigate to https://login.microsoftonline.com
3. Enter the Microsoft UPN for the test user
4. You will be redirected to the organisation's page, which is the Skolon login page.
5. Enter your Skolon credentials, either username and password or by scanning your Skolon Pass
6. You will be successfully logged into Microsoft.

Using Skolon Pass to Sign in to Windows devices

If you want to use Skolon Pass as a sign-in method to Windows devices, further configuration is required. Next steps are described in the article Configure Windows devices to use Skolon Pass

Move users to the federated domain

Once you've tested the sign-in flow successfully and followed the instructions as stated above for configuring Windows devices to use Skolon Pass as sign-in method you're ready for production.

To enable Skolon Pass as an IdP you have to make sure that the users are placed in a federated domain in Entra. There are two ways to accomplish this depending on what your setup requires:

1) If you want all users in an entire domain to use Skolon Pass as an IdP

Federate that particular domain by following the steps described in "Federating a domain"

2) If you want a sub-set of users in a domain to use Skolon Pass as an IdP

Move the concerned users to the domain you created and federated in Step 2.

If you require assistance in moving a subset of your users to a federated domain - reach out to the Skolon Support and we'll provide you with assistance.