SAML/OIDC Integration

Integration Between Azure Active Directory and Forma Cloud via SAML or OIDC

1. Introduction

The integration between **Forma LMS** and **MS Entra** (Formerly Azure Active Directory - AAD) allows users to authenticate into the learning platform using their corporate Office 365 credentials. Access is managed through standard federation protocols — **SAML 2.0** or **OpenID Connect (OIDC)** — ensuring security, centralized user management, and Single Sign-On (SSO).

---

2. Prerequisites

- An active **Entra/AAD** (Microsoft 365 / Office 365) instance.
- Administrator access to the **MS Entra portal** to create and configure enterprise applications.
- Administrator access to the **Forma LMS** instance.
- The **SAML** or **OIDC authentication plugin** installed and enabled in Forma LMS.

---

3. Choosing the Authentication Protocol

Protocol	Description	Typical Supported IdPs
SAML 2.0	XML-based standard protocol widely used for enterprise Single Sign-On.	Azure Active Directory, Microsoft ADFS, Google Identity, Auth0, SimpleSAMLphp
OIDC (OpenID Connect)	OAuth 2.0–based protocol, more lightweight and modern, ideal for cloud integrations.	Azure Active Directory, Salesforce, Auth0

> **Note:** For Microsoft 365 environments, either SAML or OIDC may be used depending on corporate security policies. Both protocols are supported by the Forma LMS authentication plugin.

---

4. Configuration via **SAML**

4.1 Creating the Application in Azure AD

1. Log in to the **Azure portal** with an administrator account.
2. Navigate to **Azure Active Directory → Enterprise Applications → New Application**.
3. Select **Create your own application** → *Non-gallery application*.
4. Enter a name, e.g., “Forma LMS SAML.”
5. Once created, go to the **Single Sign-On** section and select **SAML** as the authentication method.

4.2 SAML Configuration

Within the SAML configuration page, set the following parameters:

- **Identifier (Entity ID)**: The Entity ID URL provided by Forma LMS (e.g., `https://yourportal/formalms/saml/metadata.php`).
- **Reply URL (Assertion Consumer Service URL)**: The endpoint where SAML assertions are sent (e.g., `https://yourportal/formalms/saml/acs.php`).
- **Logout URL (optional)**: `https://yourportal/formalms/saml/logout.php`.

User Attributes Mapping

In the Azure AD application, configure the following attribute mappings:

SAML Attribute Name	Azure AD Source Attribute	Description
`username`	`user.userprincipalname`	Unique username
`givenName`	`user.givenname`	First name
`surname`	`user.surname`	Last name
`email`	`user.mail`	Email address

> Additional attributes can be sent, but only those listed above are natively managed by the Forma LMS plugin.

4.3 User Management

- **Automatic Account Creation**: Forma LMS can automatically create a user account upon first SAML login if the option is enabled in the plugin settings.
- **Data Synchronization**: User data (name, surname, email) can be updated automatically at every login.
- **Access Restriction by Organization Node**: SAML login can be restricted to users belonging to a specific organization node or sub-node.

4.4 Assigning Users or Groups

In the Azure portal, within the SAML application:

- You can **enable all Entra/Azure AD users** or **limit access to specific groups or subgroups**.
- This configuration is managed from the **Users and Groups** section of the Azure application.

---

5. Configuration via **OIDC**

5.1 Creating the OIDC Application in Azure AD

1. Log in to the Azure portal.
2. Go to **Entra/Azure Active Directory → App Registrations → New Registration**.
3. Configure:
   - **Name**: “Forma LMS OIDC”
   - **Supported account types**: “Accounts in this organizational directory only.”
   - **Redirect URI**: `https://yourportal/formalms/oidc/callback.php`.
4. After creation, note the following values:
   - **Client ID**
   - **Tenant ID**
   - **Client Secret** (generated under *Certificates & Secrets*)

5.2 Configuration in Forma LMS

In the Forma LMS OIDC plugin, enter the following parameters:

Parameter	Example Value
Client ID	`xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`
Client Secret	`**********`
Issuer URL	`https://login.microsoftonline.com/<tenant-id>/v2.0`

Parameter	Example Value
Redirect URL	`https://yourportal/formalms/oidc/callback.php`
Scopes	`openid profile email`

As with SAML, automatic account creation and user data synchronization can be enabled at login.

6. Compatibility

Protocol	Identity Providers Tested with Forma LMS
SAML	Microsoft Azure AD, Microsoft ADFS, Google Identity, Auth0, SimpleSAMLphp
OIDC	Microsoft Azure AD, Salesforce, Auth0

7. Useful Resources

- Microsoft Documentation – SAML SSO Configuration
- Microsoft Documentation – OIDC Protocol

Revision #4
Created 2025-07-01 08:46:45 UTC by Alberto Pastorelli
Updated 2025-11-13 10:12:23 UTC by Alberto Pastorelli