pangeanic

How to integrate Azure AD login in Ubuntu 23.04.

At **Pangeanic,** as an **ISO 27001 certified company**, we have always placed a high priority on security. Working in a hybrid environment where some employees work remotely and others in the office, we have strict requirements to ensure the safety of our data. The classic Active Directory solution with LDAP protocol is now considered legacy. We have been eagerly anticipating native authentication between Azure AD and Ubuntu, and with the release of Ubuntu 23.04 OS by Canonical, the company behind Ubuntu, we now have access to a range of new features designed to meet the needs of remote workers. One of the most significant new features is the integration of Azure Active Directory accounts for logging in. This integration provides an additional layer of security for our users, allowing them to authenticate using their Azure AD credentials, which are centrally managed by our IT department. How to configure Ubuntu you can find it in **this video**.

However the **configuration of Azure AD application** is not explained, we would like to share with you our manual below.

1- Creating an azure application:

To begin with, it is essential to create an Azure application to enable Azure Active Directory (Azure AD) authentication for Ubuntu.

Home > App registrations >

Register an application ⋯

* Name

The user-facing display name for this application (this can be changed later).

Canonical Login ✓

Supported account types

Who can use this application or access this API?

◉ Accounts in this organizational directory only (Pangeanic B I Europa SL only - Single tenant)

◯ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

◯ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

◯ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ⌄ | e.g. https://example.com/auth ✓

2- Giving the application the required permissions:

- Once you have created the Azure application, you need to give it the necessary permissions to authenticate with Azure AD.

- In the Azure portal, navigate to the "API permissions" section of your Azure application and grant the required permissions.

Home > App registrations > Canonical Login

Canonical Login | Authentication ⚲ ···

🔍 Search «

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- **Authentication**
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners

🗨 Got feedback?

⦿ Accounts in this organizational directory only (Pangeanic B I Europa SL only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

⚠ Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.

×

Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows:

- App collects plaintext password (Resource Owner Password Credential Flow) Learn more⤢
- No keyboard (Device Code Flow) Learn more⤢
- SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more⤢

Yes | No

Home > App registrations > Canonical Login

Canonical Login | API permissions ⚲ ···

🔍 Search «

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles

↻ Refresh | 🗨 Got feedback?

ⓘ The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configure include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission   ✓ Grant admin consent for Pangeanic B I Europa SL

API / Permissions name	Type	Description	Admin consent req...	Status
∨ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	✔ Granted

3

3- Assign the user to the enterprise application:

- After granting the necessary permissions, you need to assign the user to the enterprise application.

- Navigate to the "Enterprise applications" section of your Azure AD, select the enterprise application you created, and assign the user to the application

Home > Enterprise applications | All applications > Canonical Login

Canonical Login | Users and groups ···
Enterprise Application

«

+ Add user/group   ✏ Edit assignment   🗑 Remove   🔑 Update cred

ℹ The application will not appear for assigned users within My Apps. Set 'visible to

Assign users and groups to app-roles for your application here. To create new app
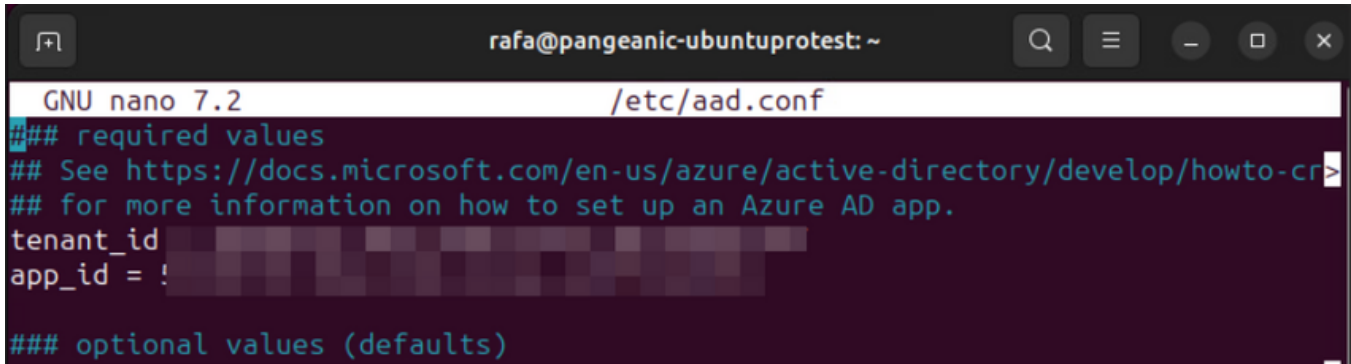
🔍 First 200 shown, to search all users & gro...

Display Name		Object Type
DA Domain Admin		User
RC Rafael Clemente Juan		User

Sidebar:
- Overview
- Deployment Plan
- Diagnose and solve problems

Manage
- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on

4- Installing the Required Packages in Ubuntu:

- In Ubuntu, install the following packages using the command: sudo apt install libpam-aad libnss-aad

- These packages enable Ubuntu to authenticate with Azure AD.

pangeanic

5- Completing the Configuration File:

- After installing the required packages, complete the configuration file with the App ID and Tenant ID from the enterprise application.

- You can find the App ID and Tenant ID in the "Overview" section of your Azure application in the Azure portal.

6- Activate the new login method:

- Next, activate the new login method by running the command: sudo pam-auth-update –enable mkhomedir.

- This command enables Ubuntu to create the home directory for the user when they first log in using Azure AD.

7- Logging in to Ubuntu with Azure Credentials:

- Finally, log in to Ubuntu using your Azure credentials.

- Click on "The user is not in the list" and enter your Azure credentials.

- If everything is set up correctly, you should be logged in to your Ubuntu desktop using your Azure credentials.!

References:

https://github.com/ubuntu/aad-auth

https://ubuntu.com/blog/azure-ad-authentication-comes-to-ubuntu-desktop-23-04

Rafa Clemente Juan
Pangeanic Support Technician