AYCC Auth User Guide

Index

1. What's AYCC Auth

2. Access to the platform
- **2.1** Initial screen
- **2.2** Access with Magic Link
- **2.3** Social login and other Identity Providers

3. User Dashboard

4. Admin Panel
- **4.1** Role and permission management
- **4.2** Identity Provider Management

5. Multi-factor authentication
- **5.1** Enabling 2FA
- **5.2** Logging with active 2FA

6. Password recovery and reset
- **6.1** Password recovery
- **6.2** Password reset

7. Customization and branding
- **7.1** Accessing the customization settings
- **7.2** Available features

8. Security and privacy

9. Conclusion and feedback

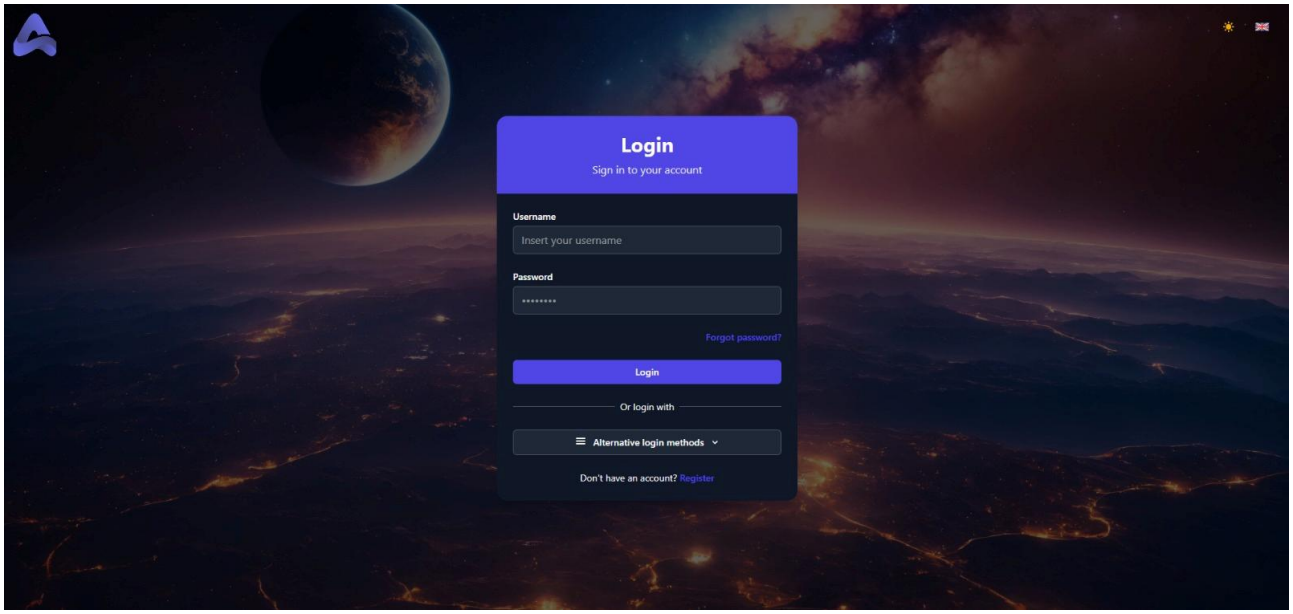
1. What's AYCC Auth

AYCC Auth is the authentication module within the AYCC ecosystem. It allows developers and organizations to securely manage user access to their digital services. Thanks to its modular architecture, AYCC Auth provides full control over identity management, permissions, and security configurations.

2. Access to the platform

AYCC Auth enables users to log in and manage their credentials in a simple and secure way.

2.1 Initial screen



When accessing AYCC Auth, users will see a login screen with the available authentication methods. From here, they can enter their email and password or choose an alternative access method.

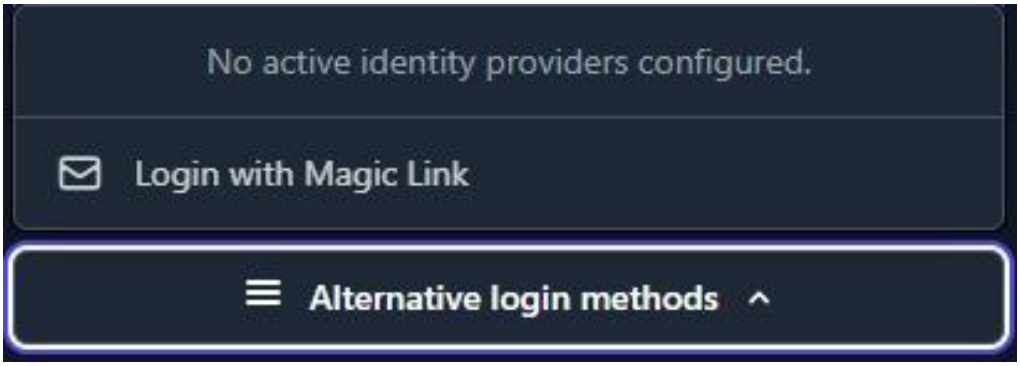
2.2 Access with Magic Link

Users who prefer a passwordless experience can choose to log in with a Magic Link. To receive it:

- Click on “Other access methods”.

- Select “Receive Magic Link”.
- Enter the registered email address.
- Open the received email and click on the login link to access the account securely.

This method increases usability and reduces the risk associated with traditional passwords.



2.3 Social login and other Identity Providers

AYCC Auth also allows access through external identity providers, such as Google, Microsoft, Facebook, or GitHub. This feature enables users to authenticate using their existing account from one of these services.

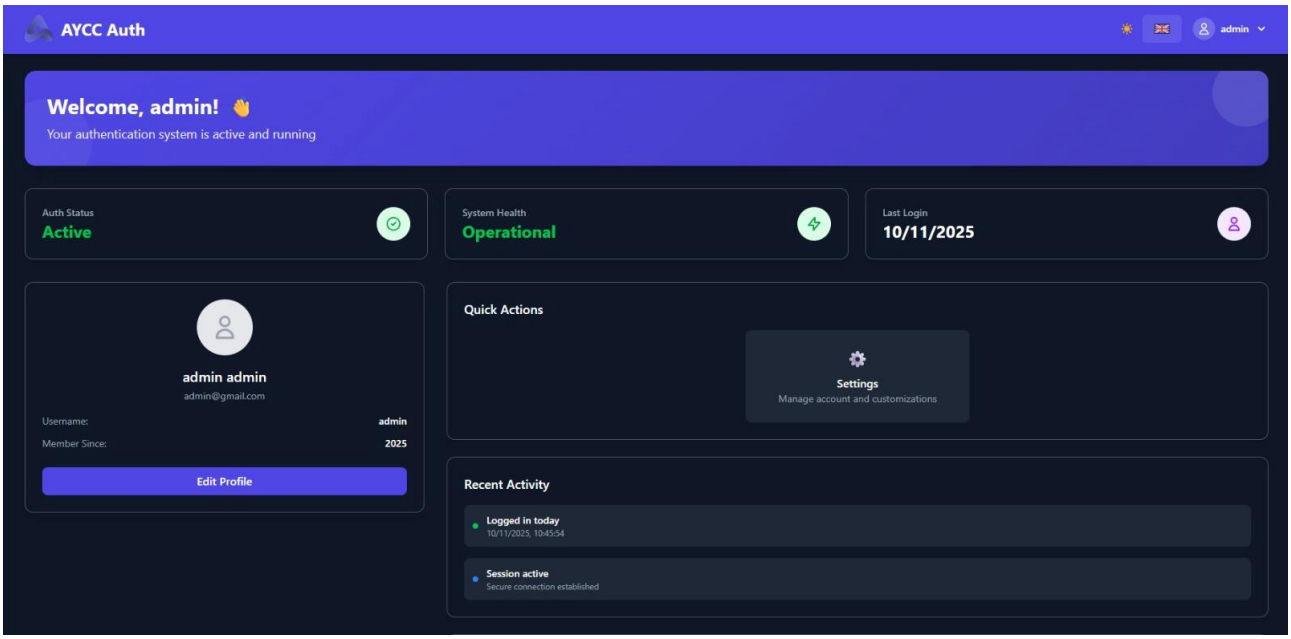
Note: The availability of these providers depends on the system configuration. Only the administrator can enable or add new providers. For more details on configuration, see section 4.2 – Identity Provider Management.

3. User Dashboard

After logging in, the user is redirected to their personal dashboard, which displays:

- Account information
- Available modules
- Security and privacy settings

From this interface, users can easily update their profile data and manage their personal preferences.



4. Admin panel

Only admins have access to this panel. The administrator panel provides access to system management functions and user permissions. To access the panel:

- From the initial screen, click on “Admin” in the upper right corner.
- A new dashboard will open with a sidebar containing several sections (Administration, Profile, Password, Groups, Roles, etc.).

4.1 Role and Permission Management

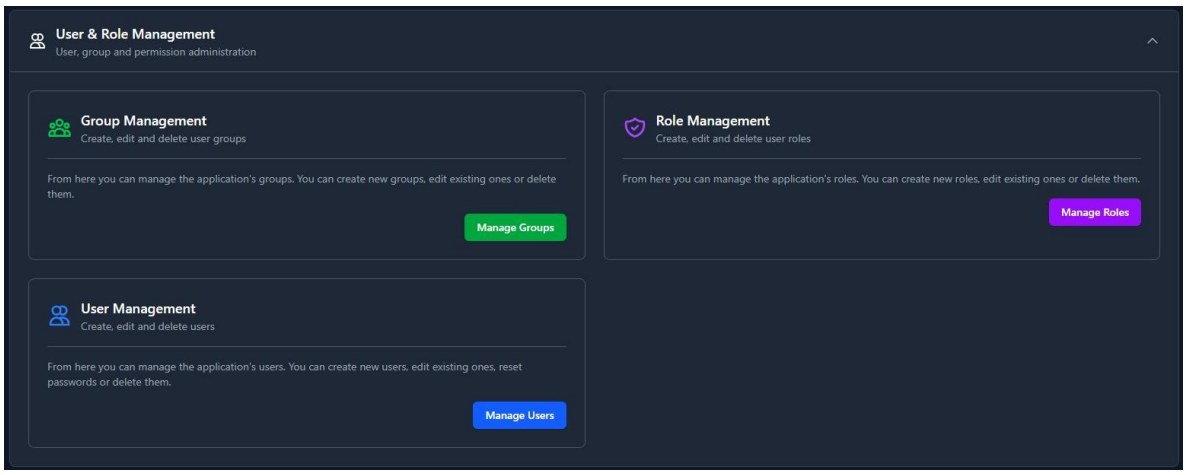
Administrators can manage user roles, permissions, and groups. To access this area:

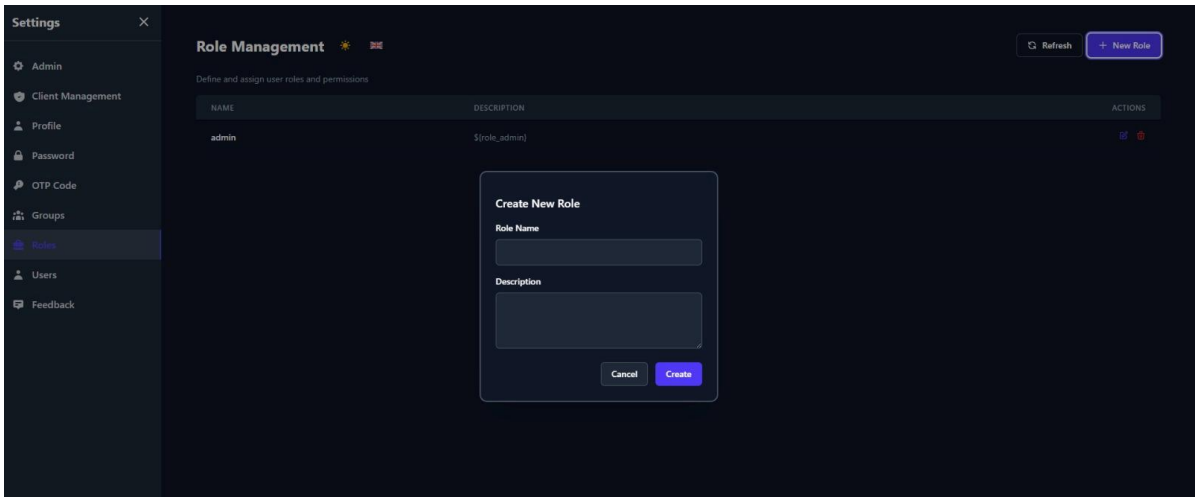
- Click on “Roles” in the left-hand menu of the admin dashboard.
- The Roles and Permissions screen will open, showing all existing roles and the users assigned to them.

From here, you can:

- Create or modify roles.
- Assign specific permissions.
- Add or remove users or groups from a role.

Each change is saved immediately and becomes effective for the associated accounts.





4.2 Identity Provider Management

In the Identity Provider section, the administrator can configure external authentication systems such as Google, Microsoft, Facebook and other OpenID Connect providers. To add a new provider:

- Open the Administration menu from the left sidebar.
- Click on Identity Providers.
- Click “Add new provider”.
- Enter the required data (client ID, secret, redirect URL, etc.).
- Save and activate the configuration.

AYCC Auth automatically integrates the new login options into the authentication screen.

5. Multi-factor Authentication

AYCC Auth supports two-factor authentication (2FA) to increase access security.

5.1 Enabling 2FA

The activation of two-factor authentication is managed at the organization level by the administrator. To enable 2FA for the organization:

- Access the Admin Panel.
- Click on Administration in the left sidebar.
- Select System Configuration.
- Enable the Two-Factor Authentication option.

Once 2FA is enabled for the organization, users will be prompted to configure it during their next login. However, each user can choose to skip this step by selecting “Skip this step” and proceed without entering an OTP. If a user later decides to activate 2FA:

- Log in to their personal account.
- Click on OTP Code in the left sidebar (the layout is similar to the admin panel but with fewer options).
- Follow the instructions to configure the OTP code:
- Scan the displayed QR code. Enter the temporary code generated by the authentication app to complete verification.

Once confirmed, two-factor authentication will be active for all future logins.

5.2 Logging in with active 2FA

If 2FA is active, after entering your credentials, you will be asked to enter the generated security code. Only after entering the correct code will access be granted.

6. Password Recovery and Reset

AYCC Auth provides a secure and simple system for recovering and resetting passwords.

6.1 Password Recovery

From the login screen, click “Forgot your password?” Enter your registered email address. Follow the link received by email to reset your password.

6.2 Password Reset

After clicking the link, you will be redirected to a page where you can set a new password. Once saved, you can log in again with your new credentials.

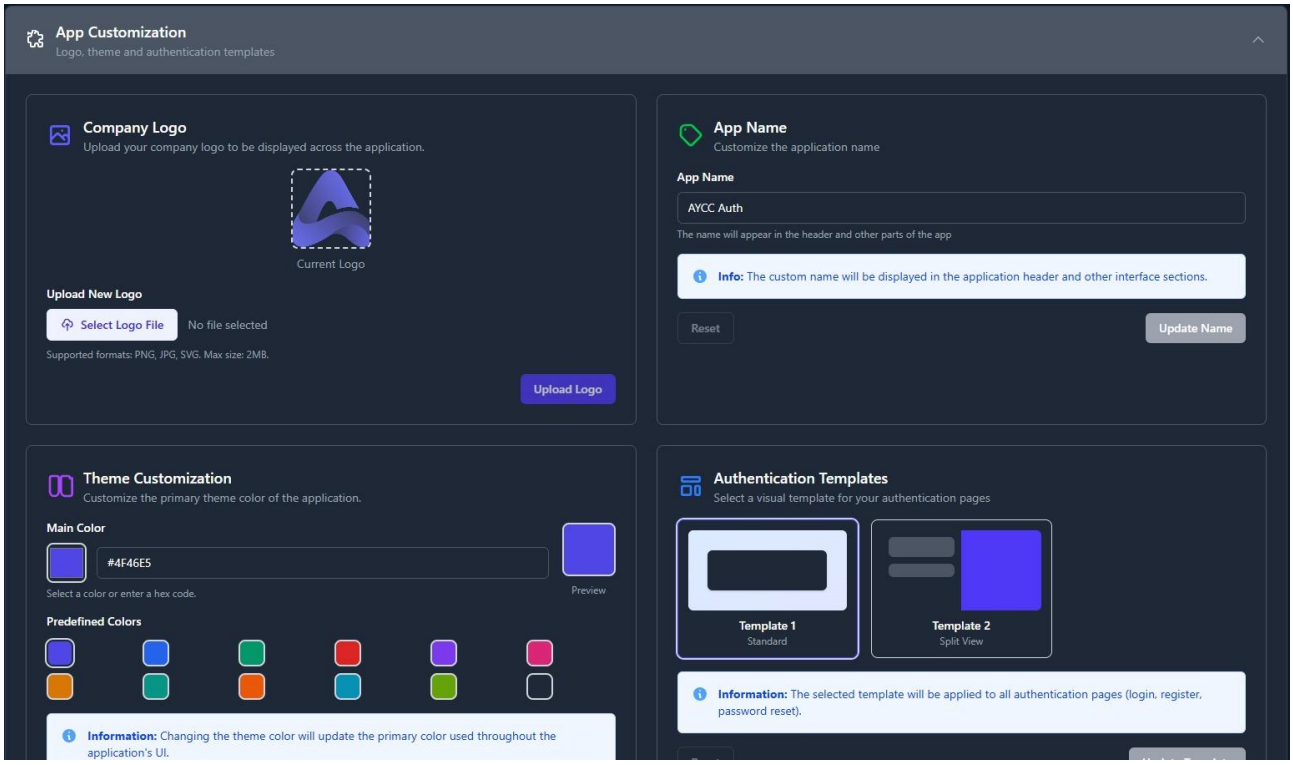
7. Customization and Branding

AYCC Auth allows you to customize the app interface with your organization's visual identity and branding. Only users with the admin role can access these settings and modify the graphical and thematic appearance of the interface. The administrator can:

- Upload the company logo
- Choose the theme (light/dark)
- Customize the main interface colors
- Set the default language

7.1 Accessing the customization settings

- From the initial screen, click on the "Admin" menu in the upper-right corner.
- In the administrative dashboard, select "Administration" from the left sidebar.
- Within the "Administration" section, open the "App Customization" menu.



7.2 Available Features

From the customization screen, you can configure the following elements:

- Company logo: upload your organization’s logo in PNG, JPG, or SVG format. The logo will appear on the login screens and in the top bar of the interface.
- Application name: define the name that will be displayed on the login screen and in notification emails.
- Theme and colors: select the preferred visual theme (light or dark) and customize the primary colors using a hexadecimal code or predefined palette. Changes are applied in real time in the preview.
- Authentication layout and templates: choose from available layouts, such as Standard or Split View, to modify the appearance of login and registration screens.
- Interface language: set the default language of the application (Italian or English).

Users can still select their preferred language from their personal profile.

8. Security and Privacy

- All communications take place over HTTPS
- Sensitive data is encrypted using AES and bcrypt algorithms
- Sessions are managed through JWT and Refresh Tokens

9. Conclusion and Feedback

AYCC Auth is a complete and intuitive solution for the secure management of access and digital identity. Designed to provide a smooth, customizable, and standards-compliant experience, it allows administrators to manage users, roles, and providers in a simple and centralized way. With AYCC Auth, everything becomes easier. This guide is constantly evolving: with the public release of the application, AYCC will collect feedback from users and system administrators to improve both functionality and documentation. The most frequent questions and most useful suggestions will be integrated into future versions of the User Guide, with the goal of making support increasingly comprehensive and up to date.

AYCC Auth