



auth-demo-example

1. [Introduction to Public Access Controls](#)
2. [SAML Authentication](#)
3. [Space-wide Password Authentication](#)
4. [Guest Accounts Authentication](#)
5. [Magic Link Authentication](#)
6. [Private Accounts Authentication](#)
7. [Private Links Authentication](#)
8. [JWT Authentication](#)

1. Introduction to Public Access Controls

Content generated with AI! For accurate information about **Public Access Control** check the [official documentation page](#).

Welcome to the Public Access Controls documentation space.

This section explains how you can manage authentication and visibility for your public-facing documentation portal. Archbee offers several authentication methods that allow you to control how readers access your content — from simple passwords to enterprise-grade SAML and JWT configurations.

Here, you will find detailed setup guides for each authentication option and learn how to apply them in your portal.

What You Will Find Here

- An overview of all available authentication methods
- Step-by-step guides for enabling each method
- Best practices for controlling access to your public documentation
- Examples and configuration tips for developers

Authentication Methods Covered

Archbee supports multiple ways to authenticate readers:

- Space-wide password
- Guest Accounts
- Magic Links
- Private Accounts
- Private Links
- JWT Authentication
- SAML Authentication

Each authentication method has its own dedicated document in this space, guiding you through configuration and usage.

Use these pages to secure your documentation portal exactly the way you need — whether you want lightweight protection or full enterprise-grade identity management.

2. SAML Authentication

This document explains how to set up and use **SAML Authentication** for your public portal.

Overview

SAML enables enterprise identity providers (Google, Azure, Okta, etc.) to authenticate visitors accessing your documentation.

How to Set It Up

1. Go to Space Settings.
2. Navigate to **Public Access Controls**.
3. Enable **SAML Authentication**.
4. Provide your IdP's metadata URL.
5. Ensure your portal is on a custom domain.

Using It in Your Portal

Users will be routed through your configured SAML provider and authenticated before viewing your documentation.

This method is ideal for enterprise-grade, centralized identity management.

3. Space-wide Password Authentication

This document explains how to use the space-wide password option to protect your public documentation portal.

Overview

A single password can be applied to your entire documentation portal. Anyone with the link and the password will gain access.

How to Set It Up

1. Go to Space Settings.
2. Navigate to Public Access Controls.
3. Enable the **Password** option.
4. Set your desired password.
5. Publish your changes.

Using It in Your Portal

When users visit your portal, they will be prompted to enter the password before accessing any content.

This is a simple and effective authentication method suitable for lightweight protection.

4. Guest Accounts Authentication

This document explains how to use **Guest Accounts** to authenticate visitors in your public portal.

Overview

Guest accounts allow you to manually create email + password combinations for your readers. These accounts do not count as seats.

How to Set It Up

1. Open Space Settings.
2. Go to **Public Access Controls**.
3. Enable **Guest Accounts**.
4. Add guest users by email.
5. Share credentials with your readers.

Using It in Your Portal

Users will log in with the email and password you assigned. Only users with guest credentials will gain access.

This method is useful when you need controlled access without complex identity management.

5. Magic Link Authentication

This document explains how **Magic Links** can be used to authenticate readers of your portal.

Overview

Magic Links authenticate users through a secure link sent to their email address.

How to Set It Up

1. Go to Space Settings.
2. Open **Public Access Controls**.
3. Enable **Magic Links**.
4. Add allowed email addresses or domains.
5. Users will receive authentication links when attempting to access the documentation.

Using It in Your Portal

Readers enter their email, receive a login link, and access the content without needing a password.

Ideal for frictionless access where password management is not desired.

6. Private Accounts Authentication

This document explains how **Private Accounts** work for authenticating users in your portal.

Overview

Private Accounts allow users to create accounts in your space using allowed email addresses or domains.

How to Set It Up

1. Open Space Settings.
2. Navigate to **Public Access Controls**.
3. Enable **Private Accounts**.
4. Add specific email addresses or domains.

Using It in Your Portal

Users whose emails match the allowed list will be able to register or log in.

Private accounts are useful when you need self-service authentication for an approved audience.

7. Private Links Authentication

This document explains how to use **Private Links** for restricting access to your documentation portal.

Overview

Private links allow you to generate unique access URLs for teams or groups. Each link corresponds to a specific audience.

How to Set It Up

1. Go to Space Settings.
2. Open **Public Access Controls**.
3. Enable **Private Links**.
4. Generate a link for each group.

Using It in Your Portal

Share the private link with the intended group. Anyone with the link will gain access.

If you want to revoke access for a group, delete its private link.

This option is ideal for managing segmented access per team or customer group.

8. JWT Authentication

This document explains how to configure and use **JWT Authentication** for your public documentation portal.

Overview

Your development team generates a JWT using a secret or JWKS key configured in Archbee. Readers authenticate via a URL containing the signed token.

How to Set It Up

1. Go to Space Settings.
2. Open **Public Access Controls**.
3. Enable **JWT Authentication**.
4. Choose between:
 - Secret-based JWT validation
 - JWKS-based JWT validation
5. Configure your server to generate the token.

Using It in Your Portal

Your system generates a URL with `?jwt=<token>&reload` appended. Users accessing that link are automatically authenticated.

JWT is recommended for automation, enterprise workflows, or large-scale user management.