Authentication in Power Pages: Architecture, Methods, and Best Practices

Abstract

This white paper provides a comprehensive overview of authentication in Microsoft Power Pages. It details the architecture, supported identity providers, security controls, and best practices for building external-facing websites. It serves as a practical guide to design robust, scalable, and user-centric authentication experiences.

Contributors:

Srinidhi VK

Bipul Deora

Contents

1. Introduction: Why authentication matters for Power Pages

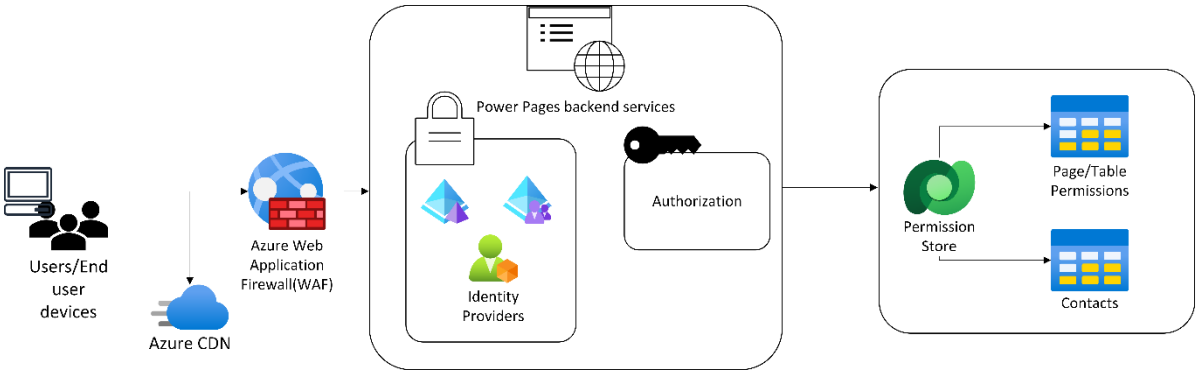
Power Pages enables organizations to create secure and scalable websites for external users, including customers, partners, vendors, citizens, and suppliers. Unlike internal business apps, these sites directly interact with people who aren't part of your organization. This aspect makes authentication a foundational pillar of the entire experience.

Whenever a user tries to access your website, you need a reliable way to verify who the user is before showing them what they're allowed to see. Authentication ensures that every visitor has a verified identity, protecting your data, your users, and your business.

In this white paper, we break down how authentication in Power Pages works, the different methods available, and the best practices to design secure, smooth, and trustworthy sign-in experiences for external users.

2. Authentication architecture

Power Pages sites run as web apps that Azure App Service hosts. These sites store their data in Dataverse, which also enforces authorization rules. Power Pages integrates with a wide range of identity providers, including Microsoft Entra ID and other external IDPs, to authenticate users. After successful authentication, the external identity is linked to a contact record in Dataverse. This mapping acts as the bridge between **authentication** (verifying who the user is) and **authorization** (determining what the user is allowed to do). Authorization is then applied based on the contact record's associated **web roles**. For Dataverse data access, this includes **table permissions** and **column permissions** that control CRUD operations on records. Additional permission models exist for other components such as Power Automate flows, business logic execution, and Web API access, each with their own authorization mechanisms.



2.1 Authentication overview

Power Pages leverages the robust ASP.NET Identity framework to handle authentication and ensures that each user is uniquely recognized and verified. It supports widely adopted authentication protocols such as:

- **OAuth2**

- **OpenID Connect (OIDC)**
- **SAML**
- **WS Federation**
- **Local Authentication**

This support provides seamless integration with various External IDPs and allows organizations to bring users from different identity systems into Power Pages.

2.2 Authorization

When users sign in successfully, their verified identity is associated to a Dataverse contact record.

Authorization rules include:

- **Web roles**, **table permissions**, and **column permissions** that define what data the user can access.
- Every time a user requests data, these permissions act as a security checkpoint, ensuring strict role-based access control.

Together, these controls provide strong, predictable, and compliant role-based access for external users.

3. Supported authentication modes

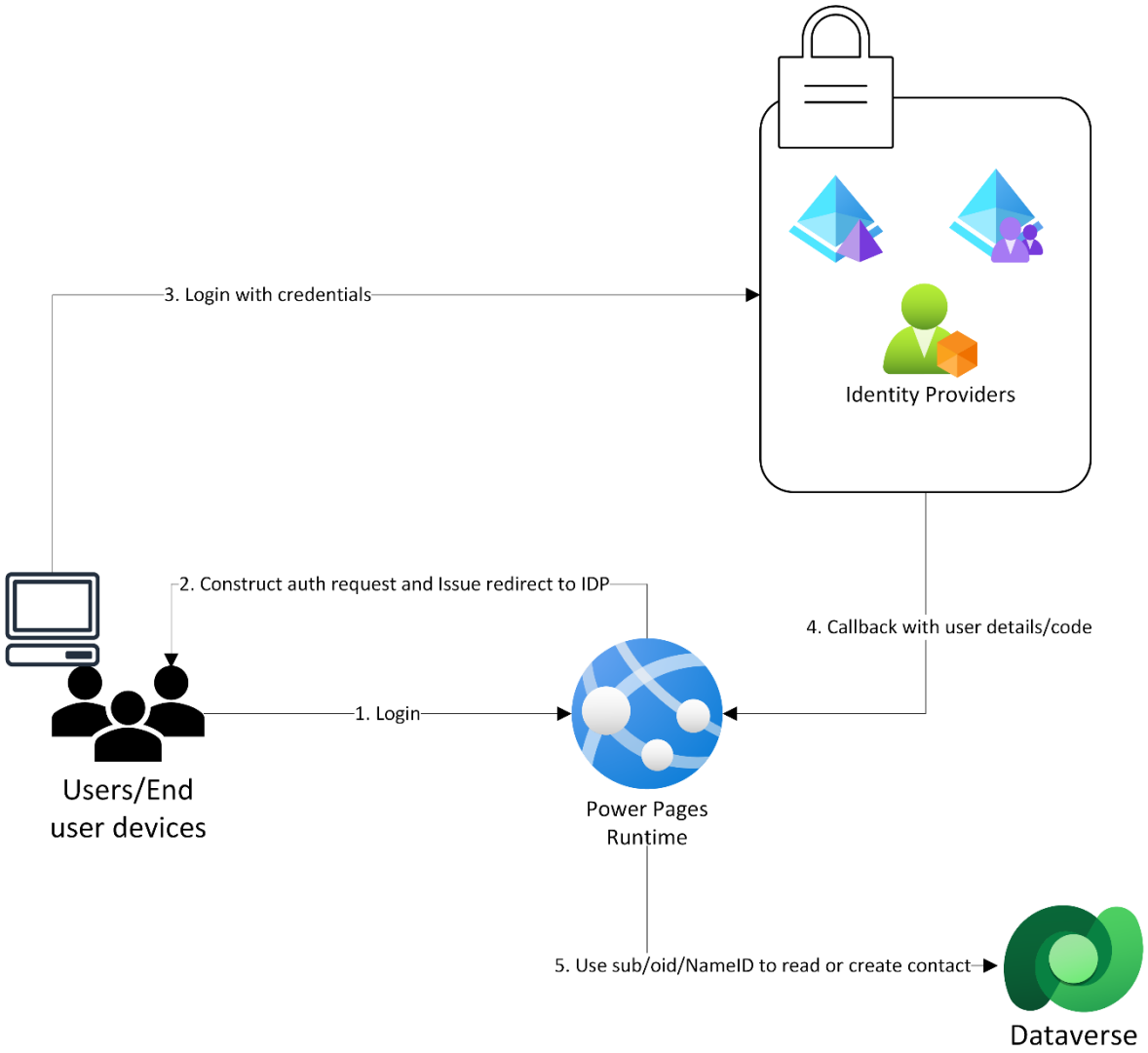
Power Pages supports multiple authentication modes to match varying business and security needs.

Method	Ideal for	Key features
OAuth 2.0	Consumer-facing portals that need familiar, low-friction sign-in	Supports Google, Facebook, Microsoft
OpenID Connect (OIDC)	Enterprises using systems like Okta, PingFederate, Auth0, or national identity systems (e.g., login.gov)	Supports custom claims mapping, full extensibility, modern protocol for identity federation
SAML	Enterprises using systems like ADFS or national identity systems (e.g., login.gov)	XML-based protocol, supports single sign-on (SSO), integrates with legacy identity systems
WS Federation	Organizations with legacy environments or apps requiring federation	Enables SSO, works with ADFS, supports claims-based authentication
Microsoft Entra ID	Internal enterprise users who authenticate using Microsoft organizational accounts	Conditional Access, MFA, identity governance, configured by default
Microsoft Entra External ID	Organizations onboarding external customers, partners, or vendors that require a federation layer across multiple IDPs	User flows, conditional access, MFA, enterprise federation

Azure AD B2C	Existing customers already using Azure AD B2C tenants	Supported for existing tenants only. On a deprecation path. No new licenses or new tenant onboarding.
Local Auth	Intended only for quick testing and not recommended for production use.	Uses ASP.NET Identity for basic username/password login.

4. Deep dive: How authentication works step-by-step

This section provides a detailed walkthrough of the end-to-end authentication flow in Power Pages. It covers the process from the moment a user initiates sign-in to the point where access is granted through Dataverse authorization.



4.1 Initiating authentication

When a user selects **Sign In**, the Power Pages runtime starts the authentication process:

- It finds the configured **Identity Provider (IDP)** for the site.
- It sends a **redirect** to the IDP's authorization endpoint with the right request parameters.

4.2 Identity provider handshake

After the redirect:

- The user authenticates with the external IDP (Microsoft Entra External ID, Okta, Auth0, ADFS, or others).
- The IDP returns an **authorization code** or **token**, depending on the protocol you choose.
- Power Pages gets this response through the configured **redirect URL** and starts validation.

4.3 Token validation and session creation

Power Pages processes tokens differently based on the chosen protocol:

OpenID Connect (OIDC) – Authorization code flow

- Exchanges the authorization code for an **ID token** (and optionally an **access token**)
- Validates *the token*

OpenID Connect (OIDC) – Other flows/OAuth 2.0 flow

- Consumes tokens returned directly in the response
- Applies standard token validation

SAML 2.0/WS Federation flow

- Processes the **SAML/WS Fed Response** posted by the IDP and applies standard token validation

Additional processing

- If configured, Power Pages queries the **UserInfo endpoint** (OIDC) to retrieve extended profile claims.
- After all validations succeed, Power Pages establishes a **secure session** and issues a **session cookie** for subsequent requests.

4.4 Contact mapping in Dataverse

Power Pages uses identity claims to map the authenticated user to a Dataverse contact:

- Claims such as *sub*, *oid*, *NameIdentifier*, or *email* are used to identify an existing contact.

- If no match is found, Power Pages creates a new contact depending on **site settings**.
- This contact becomes the **security principal** that drives authorization.

4.5 Authorization enforcement

Once the user's identity is linked to a contact:

- **Web roles** assigned to the contact determine the user's role in the site.
- **Table permissions** enforce fine-grained access to Dataverse tables and records.
- **Column permissions** restrict visibility and updates at the column level within tables.
- Every request made by the user includes the mapped contact context.
- Power Pages evaluates all permissions before returning or writing data.

4.6 Session validation, management, timeouts and sign-out

Power Pages manages the lifecycle of authenticated sessions as follows:

- Each incoming request includes the **session cookie**, which Power Pages validates.
- Site settings control session lifetime and idle timeout behaviors.
- **Idle Timeout** ends the session after a period of inactivity.
- **Absolute Timeout** ends the session after a maximum duration, regardless of activity.
- On sign-out or timeout Power Pages clears the session cookie and invalidates server-side session state.
- Power Pages supports both Service Provider initiated and IdP-initiated logout flows to ensure consistent sign-out across federated systems:
    - Service Provider initiated logout: Signing out from Power Pages triggers a logout request to the IdP.
    - IdP-initiated logout: If the user signs out directly from the IdP, the IdP notifies Power Pages, which then clears the session and completes the logout flow.

4.7 Invitation codes

Invitation-based authentication supports controlled, pre-approved onboarding to a Power Pages site

- Invitation codes are validated before contact creation.
- Codes can enforce expiration, single-use, or contact-based mapping.
- After a user redeems an invitation:
    - Their identity maps to the corresponding Dataverse contact.
    - They proceed through the standard authentication flow.

5. Common scenarios and best practices

This section outlines the most frequent authentication scenarios encountered in Power Pages and provides recommended configurations based on industry patterns and platform capabilities.

5.1 Common scenarios

Scenario	Recommended method	Common Site settings pattern
Customer self-service portal requiring social login	OIDC (For example, Facebook or Google)	*RegistrationEnabled = true; OpenRegistrationEnabled = true; InvitationEnabled = false*
Partner collaboration site allowing access via all partner IDPs	Microsoft Entra External ID (OIDC), Okta, Auth0	*RegistrationEnabled = true; OpenRegistrationEnabled = true; InvitationEnabled = false*
Vendor onboarding with restricted invitation access	Microsoft Entra External ID, Okta	*RegistrationEnabled = true; OpenRegistrationEnabled = false; InvitationEnabled = true;*
Government / NGO portal requiring integration with national IDPs and pre-created contacts	SAML or OIDC with custom IDP like login.gov, Singpass	*RegistrationEnabled = false; OpenRegistrationEnabled = false; InvitationEnabled = false;*
Internal HR / IT self-service portal for employees using enterprise identity	Microsoft Entra ID or Okta (OIDC)	*RegistrationEnabled = true; OpenRegistrationEnabled = true; InvitationEnabled = false;*

Note: These settings are indicative only and represent common patterns. Additional configuration such as identity provider setup, external login enablement, user flows, and claims mapping is also required based on the scenario.

5.2. Best practices

The following best practices help ensure secure, predictable, and compliant authentication behaviour across Power Pages sites.

5.2.1. Enforce strong security

- **Enable MFA** for all sensitive portals by using Microsoft Entra External ID or your IDP's MFA capabilities.

- Set **NonceLifetime** to the shortest duration needed to complete authentication between Power Pages and the IDP.

5.2.2. Control registration behavior

- **Invitation-only portals**:
    - Set *OpenRegistrationEnabled=false* and *InvitationCodeRequired=true* for controlled onboarding.
- **Pre-provisioned users**:
    - If you create all contacts in advance, set *RegistrationEnabled=false* to prevent accidental sign-ups.
- **Restrict legacy mechanisms**
    - Disable **Local Login**, as it doesn't meet modern security standards. It should be used only for demos or testing.

5.2.3. Manage identity mapping carefully

- Always use the default identity mapping, which uses identifiers (*sub*, *oid*, or *NameIdentifier*) to identify contact.
- Use *AllowContactMappingWithEmail=true* **only during migration**, then disable it after migration.
- Ensure Dataverse contacts are updated with IDP claims by using claims mapping to maintain integrity.

5.2.4. Protect registration and sign-in pages

- Require acceptance of **Terms & Conditions** during registration to meet regulatory and compliance requirements.
- Use clear branding and distinct IDP labels to reduce confusion and improve the user experience.

5.2.5. Secure session management

Configure idle and absolute timeouts to reduce the risk of hijacked sessions. Ensure session timeout values at the IDP and Power Pages are aligned and enable SP-initiated logout to enforce consistent sign-out behaviour.

Setting	Description	Default value
Idle Timeout (Authentication/ApplicationCookie/ExpireTimeSpan)	Terminates the session after a defined period of inactivity.	24:00:00 (24 hours) Syntax: HH:MM:SS

Absolute Timeout (Authentication/ApplicationCookie/AbsoluteSlidingExpireTimeSpan)	Ends the session after a maximum allowable duration, regardless of user activity.	NA

6. Advanced configuration options

Power Pages offers a range of advanced configuration capabilities designed for enterprise environments that require granular control over authentication, security, and identity lifecycle management.

6.1 Identity migration in Power Pages

Power Pages supports structured migration approaches for organizations transitioning users from legacy identity systems to modern platforms such as Microsoft Entra External ID. The following strategies ensure continuity while avoiding duplicate contacts and inconsistent authorization mappings.

1. Pre-provisioned contact records

- Create Dataverse contact records before users begin signing in.
- Add **External Identity** records mapped to provider keys such as *sub*, *oid*, or *NameIdentifier*.
- Assign web roles and related permissions in advance.

2. Invitation-based migration

- Generate invitations for each pre-created contact.
- Enforce expiration and single-use constraints as required.
- Users redeem invitations, ensuring precise mapping between their external identity and the correct Dataverse contact.

3. Email-based contact mapping

- Temporarily enable **AllowContactMappingWithEmail = true** during migration.
- Allows incoming identities to be matched to contacts based on email.
- Disable this setting after all users authenticate at least once, restoring *sub*, *oid* or *NameIdentifier* as the mapping keys.

6.2 OpenID advanced parameters

When using OpenID Connect, Power Pages can use advanced parameters to align authentication flows with organizational policies or assurance requirements.

Parameter	Function	Example
scope	Specifies the claims required by the application.	openid profile email

prompt	Governs whether the user should reauthenticate or whether silent authentication is allowed.	login, none
acr_values	Indicates the authentication assurance level required by the application.	MFA, urn:mace:incommon:iap:silver

These parameters give you control over claim issuance, reauthentication rules, and assurance enforcement in federated sign-in scenarios.

6.3 Multiple identity providers

Power Pages supports integration with multiple identity providers, so diverse user groups can authenticate by using their preferred or mandated identity platform.

Configuration requirements:

- Set **ExternalLoginEnabled = true**.
- Add and configure the required identity providers, which might include:
  - Microsoft Entra External ID
  - OAuth/OIDC providers such as Google, LinkedIn, or Facebook
  - SAML 2.0 identity providers including Okta, PingFederate, or ADFS

This approach accommodates hybrid authentication models that span consumer, partner, and enterprise identity systems.

6.4 Claims mapping

Power Pages provides a way to copy IDP attributes into the Power Pages contact record using *claims mapping*. Claims mapping can be applied **once during registration** using *registration claims mapping*, or it can be updated every time the user logs in using *login claims mapping*.

Power pages supports claims mapping from token directly and additionally from userinfo endpoint for OpenId protocol based IDPs.

6.5 Use custom claim for email

By default, Power Pages identifies the email address to use for contact creation by referencing claims such as *email*, *emails*, and *upn*. You can tailor this behavior by configuring the following setting.

Setting	Description
Email claim identifier (Authentication/{Provider}/{ProviderName}/EmailClaimIdentifier)	Uses the specified claim name to identify the contact email.

6.6 Customize Sign In page

Power Pages allows you to customize the sign-in page appearance and messaging through content snippets and CSS. You can modify headings, button labels, information messages, and visual styling to match your brand without code changes.

Available Content Snippets

Snippet name	Description
Account/SignIn/SignInExternalFormHeading	Main heading displayed above external authentication provider buttons
Account/SignIn/PageCopy	Descriptive text displayed at the top of the sign-in page. This can also be used to add custom CSS styles, html elements and change the experience.
Account/Register/RegistrationDisabledMessage	Message shown when external registration is disabled
Account/SignIn/IdentityProviderTitle	Tooltip text for provider buttons (supports {0} placeholder for provider name)
Account/Redeem/InvitationCodeAlert	Message displayed when redeeming an invitation code

6.7 Configure Default Identity Provider

Power Pages supports setting up default identity provider in security workspace experience.

7. Security, governance, and compliance

Power Pages authentication is built on Microsoft's enterprise security stack and operates within a Zero Trust framework, ensuring all identities, sessions, and requests are explicitly validated. TLS 1.2+, secure cookies, hardened session lifecycles, and Dataverse-backed authorization protect all authentication flows and ensure end-to-end protection for external users.

Administrators have strong governance controls to secure authentication and access. Website visibility defaults to *Private*, preventing unintended exposure, and admins can enforce strict onboarding models by using settings like **OpenRegistrationEnabled,** and **InvitationEnabled.** Additional governance controls to enable or disable external authentication providers and disable anonymous access entirely for websites that require authenticated entry. Authorization remains tightly governed through web roles, page permissions, and table permissions, ensuring least-privilege access to all business data. Power Pages further integrates with IP restrictions, Azure Web Application Firewall, audit logging, and Application Insights, enabling monitoring of failed sign-ins, anomaly detection, and alignment with compliance standards such as GDPR, ISO, SOC, and FedRAMP.

Together, these controls establish a secure, governed, and compliant authentication model that gives organizations confidence when extending business data and processes to external users.

For a detailed overview of Power Pages security architecture, governance model, and compliance certifications, see the *Power Pages Security Whitepaper.*

9. Conclusion

Power Pages provides a comprehensive and extensible authentication framework that supports modern identity standards and integrates seamlessly with enterprise, consumer, and custom identity providers. By combining trusted identity platforms with Dataverse-based authorization, organizations can deliver secure, scalable, and user-centric external experiences. The approaches and configurations outlined in this white paper enable makers, developers, and architects to implement authentication confidently and align portal access with organizational security and compliance requirements.