

Understanding Authentication Methods in ID Everywhere

Overview

ID Everywhere provides centralized identity management so users can authenticate to supported applications using their ID Everywhere credentials.

Different applications support different authentication technologies. Understanding these technologies helps you choose the correct integration method.

ID Everywhere currently provides two documented integration methods:

- **OpenID Connect (OIDC)** for modern applications that support identity-provider-based sign-in.
- **LDAP** for applications that authenticate users through a directory service.

These methods serve different purposes, but both can use ID Everywhere as the authoritative source for user authentication.

What is OpenID Connect (OIDC)?

OpenID Connect is an identity authentication protocol built on OAuth 2.0.

It allows an application to redirect a user to a trusted identity provider, such as ID Everywhere, to complete sign-in.

How OIDC works

1. A user opens an application that is configured to use ID Everywhere.

2. The application redirects the user to ID Everywhere.
3. ID Everywhere authenticates the user.
4. After successful authentication, the user returns to the application.
5. The application securely validates the authentication response and identifies the signed-in user.

The application does not need to collect or store the user's ID Everywhere password.

Common OIDC use cases

- Web applications with an external identity-provider option.
- Custom business applications.
- Mobile and desktop applications that support OIDC.
- Applications offering configurable OpenID Connect single sign-on.

Choose OIDC when the application explicitly supports OpenID Connect or a compatible custom OIDC identity provider.

What is OAuth 2.0?

OAuth 2.0 is an authorization framework that allows applications to obtain tokens for permitted access.

OIDC uses OAuth 2.0 as its foundation and adds standardized user identity information.

This distinction is important:

- **OAuth 2.0:** Primarily provides authorization.
- **OIDC:** Provides authentication and identity information using OAuth 2.0 mechanisms.

An application advertising OAuth 2.0 support does not necessarily support OIDC sign-in.

ID Everywhere currently supports the **Authorization Code** grant for its OIDC integration.

Support for OIDC does not automatically mean ID Everywhere supports every OAuth 2.0 grant type.

What is LDAP?

Lightweight Directory Access Protocol (LDAP) is commonly used by applications that need to look up directory users and verify credentials.

Unlike OIDC, LDAP generally does not involve redirecting the user's browser to an identity provider. Instead, the application communicates with a directory service.

How LDAP authentication works with ID Everywhere

1. An LDAP-compatible application connects to the configured directory service.
2. The application submits a user authentication request.
3. The LDAP service delegates password verification to ID Everywhere.
4. ID Everywhere evaluates the credentials and account status.
5. The LDAP service returns an authentication result to the application.

ID Everywhere remains the authoritative password provider. The LDAP integration does not maintain a separate database of end-user passwords.

Common LDAP use cases

- Email applications supporting LDAP authentication.
- Legacy business applications.
- Software that requires directory-based user verification.
- Applications that can search an LDAP directory for user information.

Use a secure LDAP connection, such as LDAPS or an appropriately configured StartTLS connection, when transmitting credentials across networks.

What about SAML, OAuth 1.0, RADIUS, and Kerberos?

These are separate authentication or authorization technologies.

Technology	Purpose	Current ID Everywhere status
OpenID Connect (OIDC)	Modern federated user sign-in	Supported
OAuth 2.0 Authorization Code	Authorization flow used by OIDC	Supported for OIDC
LDAP	Directory access and authentication	Supported
OAuth 1.0	Older authorization protocol	Not supported by the documented integration

SAML 2.0	Enterprise federated authentication	Not currently supported
RADIUS	Network access authentication	Not currently supported
Kerberos	Ticket-based network authentication	Not currently supported

Other OAuth 2.0 grants, including Client Credentials, Implicit, Resource Owner Password Credentials, and Device Authorization, are not part of the currently documented IDE integration.

How do I choose the correct method?

Start by reviewing the application's authentication or SSO settings.

If it supports OpenID Connect: Configure an OIDC application in ID Everywhere.

If it supports LDAP: Configure an LDAP integration using the appropriate directory connection information.

If it only supports SAML, RADIUS, Kerberos, or OAuth 1.0: Do not attempt to configure it as OIDC or LDAP. Those protocols are not interchangeable.

If it says only "OAuth 2.0": Confirm that it supports OIDC authentication, an ID token, and a custom OIDC provider.

Frequently asked questions

Can one user use both OIDC and LDAP?

Yes. A user may authenticate to different compatible applications through either integration, subject to account status and applicable access controls.

Does an OIDC application receive the user's password?

No. The user authenticates with ID Everywhere. The application receives an authorization response and tokens, not the user's password.

Does LDAP maintain a separate password?

No. ID Everywhere's LDAP architecture delegates password verification to ID Everywhere.

Does every application support ID Everywhere?

No. The application must support an authentication method that ID Everywhere provides.

Related articles

- [Choosing the Right OIDC Application Type](#)
- [Connecting an Application Using OIDC](#)
- [Understanding OIDC Settings and Security Terms](#)

Revision #2

Created 2026-10-10 22:08:04 UTC by Administrator

Updated 2026-10-10 22:10:21 UTC by Administrator