

Identity standards, demystified

How modern web apps authenticate users and access APIs

STANDARDS, IDPS, AND THE TYPICAL LOGIN FLOW

General educational guidance, not affiliated with or endorsed by any standards body or vendor named. Standards and vendor support change, so confirm a detail before you depend on it. Published 2026-07-13.

3 problems to solve

authentication, authorization, provisioning

6 standards in active use

SAML 2.0 • OpenID Connect • FIDO2/WebAuthn • OAuth 2.0 • Token Exchange • SCIM 2.0

01 Authentication, proving who the user is

"Are you the right person?" The IdP verifies identity and tells the app.

AUTHN • WHO YOU ARE

SAML 2.0

OASIS Standard, March 2005. XML-based assertions.

SAML is what enterprise IT teams configure when they want their employees to sign in to your app using their corporate identity. Common in regulated industries and large enterprises.

OpenID Connect (OIDC)

OpenID Foundation, 2014. ISO/IEC 26131:2024. JSON/JWT identity layer on OAuth 2.0.

Modern login. Adds an ID token (a JWT) and a UserInfo endpoint for extra profile data to OAuth 2.0. The default choice for new web apps, mobile apps, and SPAs.

FIDO2 / WebAuthn (passkeys)

W3C Recommendation, WebAuthn Level 2 (2021), FIDO Alliance CTAP. Public-key cryptography.

Phishing-resistant credential. Replaces or strengthens passwords using a key pair bound to the device. The basis for passkeys across Apple, Google, and Microsoft ecosystems; CTAP is the companion protocol that lets a phone or security key talk to the browser.

02 Authorization, granting access without sharing credentials

"What can this app do on the user's behalf?" Tokens scope the access.

AUTHZ • WHAT YOU CAN DO

OAuth 2.0

IETF RFC 6749, October 2012. Delegated access via access tokens.

Lets an app call an API on the user's behalf without seeing their password. Used by Microsoft Graph, Google APIs, and most modern API integrations. Authorization, not authentication.

OAuth 2.1 (in progress)

IETF Working Group draft. Consolidates OAuth 2.0 with security best practices.

- Makes PKCE mandatory.
- Removes the Implicit and Resource Owner Password Credentials flows.
- Forbids bearer tokens in URL query strings.
- Intended to supersede OAuth 2.0 once finalized.

OAuth 2.0 Token Exchange

IETF RFC 8693, January 2020. Security token exchange.

Service-to-service identity propagation. Lets a service swap one token for another with narrower scope or different audience. Used by microservices and AI agents that must call APIs as the original user.

03 Provisioning, keeping the directory in sync

"Who exists, and what changed?" Automatic user lifecycle across systems.

SYNC • WHO EXISTS

SCIM 2.0

IETF RFC 7642/7643/7644, September 2015. REST/JSON user provisioning.

Creates, updates, and deactivates accounts across systems, where both sides support SCIM. When HR adds a hire to your IdP, SCIM pushes that user into Salesforce, Slack, and other connected apps.

04 The Identity Provider layer

An IdP is the system that authenticates users and issues tokens. The standards above define how it talks to your app.

IDP • WHO ISSUES TOKENS

Microsoft Entra ID

SAML 2.0, OIDC / OAuth 2.0, SCIM 2.0, FIDO2 passkeys (device-bound and synced).

Microsoft recommends OIDC for new apps. WS-Federation, an older Microsoft federation protocol, remains supported for existing integrations.

Google Workspace

SAML 2.0, OIDC, OAuth 2.0, SCIM 2.0 (Cloud Identity auto-provisioning), FIDO2 / passkeys.

SSO profiles support custom OIDC IdPs and SAML. Pre-configured profile available for Entra ID.

Other major IdPs

Okta, Ping Identity, Auth0, OneLogin, and JumpCloud all support SAML 2.0, OIDC, OAuth 2.0, SCIM 2.0, and FIDO2/WebAuthn. Token Exchange support varies by vendor.

05 A typical web app authentication flow

User logs in once, app gets identity, then calls APIs on the user's behalf.



PRACTICE

Identity standards in practice

Worked examples, shared vocabulary, common pitfalls, and how to choose

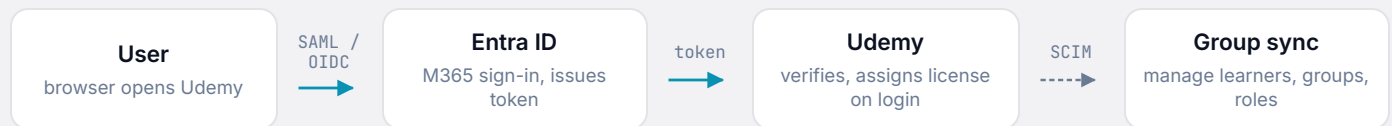
06 Integration examples

Four common patterns connecting external apps and pipelines to Microsoft Entra ID.

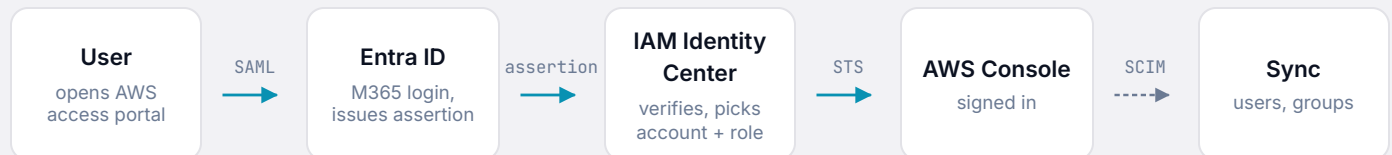
KnowBe4 + Microsoft Entra ID SAML 2.0 SSO with SCIM 2.0 user provisioning.



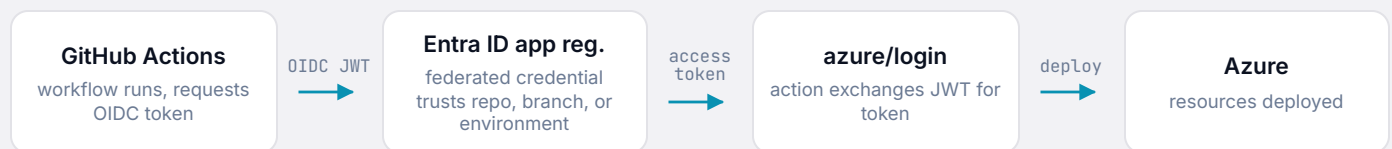
Udemy Business + Microsoft Entra ID SAML 2.0 or OIDC for SSO plus SCIM 2.0 (both Enterprise Plan only).



AWS Management Console + Microsoft Entra ID SAML 2.0 to AWS IAM Identity Center with SCIM 2.0.



GitHub Actions + Azure (CI/CD authentication) OIDC with workload identity federation. No stored secrets.



Replaces long-lived service principal secrets. Subject is constrained to a specific repo, branch, tag, or environment.

Cyan solid arrows are the live sign-in or auth flow. Grey dashed arrows are SCIM provisioning.

07 Glossary

Shared vocabulary for the protocols and roles above.

IdP, Identity Provider

The system that authenticates users and issues tokens. Entra ID, Okta, Google.

SP, Service Provider

The app the user is logging into. KnowBe4, Udemy, AWS. The receiver of the assertion.

RP, Relying Party

OIDC's name for the SP. Same role, different vocabulary.

Assertion, claim

A signed statement from the IdP about the user (email, name, group).

JWT, JSON Web Token

RFC 7519. The compact, signed JSON format used by OIDC and OAuth.

PKCE, Proof Key for Code Exchange

RFC 7636. Stops auth-code interception. Mandatory in OAuth 2.1.

JIT, Just-in-Time provisioning

The app creates the account at first login. Quick to set up; it never deactivates anyone (see the pitfalls).

STS, Security Token Service

A token-issuing service; RFC 8693 uses the term for the token-exchange role. AWS STS, the issuer of temporary credentials, is the last hop in the AWS Console flow above.

08 These are not standards

Common terms that name an experience or pattern, not a wire protocol.

SSO, Single Sign-On

A user experience, delivered by SAML or OIDC.

MFA, Multi-Factor Authentication

A security category, implemented by FIDO2, TOTP, push, or SMS.

Federation

A trust pattern between organizations or tenants.

Zero Trust

An architecture and philosophy described in NIST SP 800-207. No single standard defines it.

09 Quick comparison

What each standard is for, what it issues, and where it fits.

STANDARD	PURPOSE	TOKEN FORMAT	BEST FOR
SAML 2.0 OASIS	Authentication Enterprise SSO	XML assertion Signed	Legacy enterprise apps, regulated industries
OpenID Connect OpenID Foundation	Authentication Modern login	JWT (ID token) JSON	New web apps, mobile, single-page apps
FIDO2 / WebAuthn W3C, FIDO Alliance	Authentication Phishing-resistant	Public key pair Device-bound or synced	Passwordless MFA, passkey rollouts
OAuth 2.0 IETF RFC 6749	Authorization Delegated API access	Access token Opaque or JWT	API integrations (Graph, Drive, etc.)
Token Exchange IETF RFC 8693	Authorization Identity propagation	Token swap JWT or opaque	Service-to-service, microservices, agents
SCIM 2.0 IETF RFC 7642/7643/7644	Provisioning User lifecycle	REST + JSON add, update, deactivate	Auto-provisioning users into SaaS apps

10 Common pitfalls

What teams most often get wrong about these standards.

- **Using OAuth 2.0 alone for authentication**

An access token proves authorization, not identity. Use OIDC for login.

- **Assuming SAML is dead**

Regulated industries and large enterprises still standardize on it.

- **Building a B2B app with only OIDC**

Many enterprise customers require SAML for SSO. Implement both protocols.

- **Treating synced passkeys as single-factor**

- When user verification (a biometric or PIN) is required, a synced passkey counts as multi-factor in policy engines such as Entra ID Conditional Access and Google Workspace.
- They can meet NIST's AAL2. AAL3, the highest tier, still requires a hardware-bound key (SP 800-63B-4).

- **Skipping SCIM and relying on JIT provisioning**

JIT creates accounts on login but never deactivates them on offboarding.

- **Saying "SCIM" without specifying a version**

SCIM 1.1 and 2.0 are not interoperable. Always verify the version.

11 Use this when...

Pick the standard that matches the situation.

New SaaS or web app needing user login

→ [OpenID Connect \(OIDC\)](#). The modern default for new apps.

Enterprise customer mandates SSO with their IdP

→ [SAML 2.0](#), the default for legacy IdPs and regulated industries, though [OIDC](#) is increasingly accepted.

App needs to call Microsoft Graph or Google APIs

→ [OAuth 2.0](#) for the API call ([OAuth 2.1](#) once finalized); use [OIDC](#) to sign the user in.

Replacing passwords with phishing-resistant MFA

→ [FIDO2](#) / [WebAuthn](#) passkeys.

CI/CD pipeline deploying to a cloud

→ [OIDC](#) with [workload identity federation](#). No stored secrets, scoped to repo or branch.

Auto-provision and deprovision users in SaaS

→ [SCIM 2.0](#).

Sign in to AWS Console with M365 credentials

→ [SAML 2.0](#) to [AWS IAM Identity Center](#), plus [SCIM 2.0](#) to keep users in sync.

Roll out training apps like KnowBe4 or Udemy

→ [SAML 2.0](#) (or [OIDC](#) if supported) plus [SCIM 2.0](#) for HR-driven user lifecycle.

Wiring AI agents or microservices to call APIs as the user

→ [OAuth 2.0](#) with [Token Exchange \(RFC 8693\)](#) where identity must propagate across service hops.

References

OASIS: SAML 2.0 standard · docs.oasis-open.org/security/saml/v2.0/

OpenID Foundation: OpenID Connect Core 1.0 · openid.net/specs/openid-connect-core-1_0.html

W3C: WebAuthn Level 2 · w3.org/TR/webauthn-2/

FIDO Alliance: FIDO2 and CTAP specifications · fidoalliance.org/specifications/

IETF: RFC 6749, OAuth 2.0 · datatracker.ietf.org/doc/html/rfc6749

IETF: OAuth 2.1 draft · datatracker.ietf.org/doc/html/draft-ietf-oauth-v2-1

IETF: RFC 8693, Token Exchange · datatracker.ietf.org/doc/html/rfc8693

IETF: RFCs 7642, 7643, 7644, SCIM 2.0 · datatracker.ietf.org/doc/html/rfc7644

IETF: RFC 7519, JWT · datatracker.ietf.org/doc/html/rfc7519

IETF: RFC 7636, PKCE · datatracker.ietf.org/doc/html/rfc7636

NIST SP 800-207, Zero Trust Architecture · csrc.nist.gov/pubs/sp/800/207/final

NIST SP 800-63B-4, Authentication and Authenticator Management · pages.nist.gov/800-63-4/sp800-63b.html

Microsoft: Entra ID app sign-in protocols ·

learn.microsoft.com/entra/identity-platform/v2-protocols

Microsoft: passkeys in Entra ID ·

learn.microsoft.com/entra/identity/authentication/concept-authentication-passwordless

Google Workspace: SSO profiles for third-party IdPs ·

knowledge.workspace.google.com/admin/apps/setting-up-sso

Microsoft: KnowBe4 SSO and provisioning tutorials ·

learn.microsoft.com/entra/identity/saas-apps/knowbe4-tutorial

Udemy Business: SSO and SCIM provisioning · business-support.udemy.com

AWS: IAM Identity Center with Microsoft Entra ID ·

docs.aws.amazon.com/singlesignon/latest/userguide/idp-microsoft-entra.html

GitHub: OpenID Connect in GitHub Actions ·

docs.github.com/actions/concepts/security/openid-connect

Microsoft: workload identity federation ·

learn.microsoft.com/entra/workload-id/workload-identity-federation