

Identity standards, demystified

How apps, pipelines, and services prove who they are and reach 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 2026-09-07.

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. Builds on OAuth 2.0, adding an ID token (a JWT) and a UserInfo endpoint for extra profile data. The default choice for new web apps, mobile apps, and single-page apps (SPAs).

FIDO2 / WebAuthn (passkeys)

W3C Recommendation, WebAuthn Level 3 (2026), 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 on Apple, Google, and Microsoft platforms. CTAP is the companion protocol that lets a phone or security key talk to the device the user is signing in on.

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. It authorizes API calls; it does not authenticate the user. Build against RFC 9700 (BCP 240, January 2025), which updates RFC 6749 and carries the security rules that apply today.

OAuth 2.1 (in progress)

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

- Requires PKCE, apart from a narrow exception for confidential clients that use the OpenID Connect nonce.
- 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. Check the vendor's plan as well as its feature list, because SaaS products often sell SCIM only on a higher tier.

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, and still supports WS-Federation, its older federation protocol, for existing integrations.

Google Workspace

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

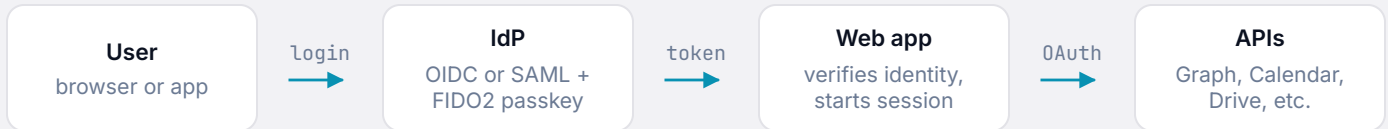
SSO profiles support custom OIDC IdPs and SAML. Google provides a pre-configured profile for Entra ID.

Other major IdPs

Okta, Ping Identity, Auth0, OneLogin, and JumpCloud all support SAML 2.0, OIDC, OAuth 2.0, and FIDO2/WebAuthn. Check the SCIM direction you need: Okta, Ping, OneLogin, and JumpCloud provision out to apps, while Auth0 only receives provisioning from an upstream IdP. 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.



SCIM runs in the background, syncing user accounts between the IdP and connected apps.

Signing out has to be configured separately. SAML Single Logout, and OIDC RP-initiated or back-channel logout, end the app session as well as the IdP session when the user signs out. Neither reaches an account an administrator disables: that app session runs until its token expires. SCIM deprovisioning closes it, and so does a revocation signal from the IdP, which Microsoft Entra ID sends as continuous access evaluation and the OpenID Shared Signals Framework standardizes.

PRACTICE

Identity standards in practice

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

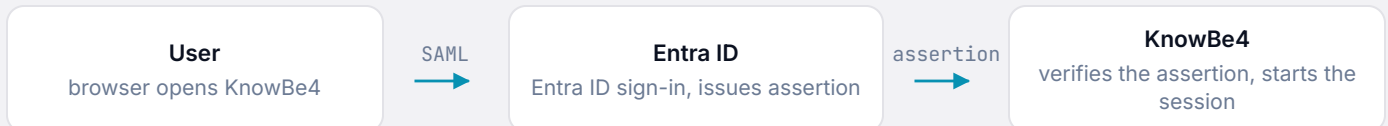
06 Integration examples

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

The arrows follow the live sign-in or auth flow. Where SCIM provisioning also runs, the note under the example says what it does.

KnowBe4 + Microsoft Entra ID

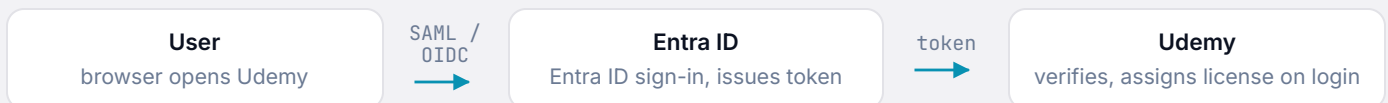
SAML 2.0 SSO with SCIM 2.0 user provisioning.



SCIM is a separate connection: Entra ID adds, updates, and archives users in KnowBe4. KnowBe4 can also create an account from the SAML login, under Allow Account Creation from SAML Login. Leave that off where SCIM provisions, so one system owns the account.

Udemy Business + Microsoft Entra ID

SAML 2.0 or OIDC for SSO plus SCIM 2.0 (both Enterprise Plan only).



SCIM is a separate connection: Entra ID provisions users and groups into Udemy, which manages learners, groups, and roles from them.

AWS Management Console + Microsoft Entra ID

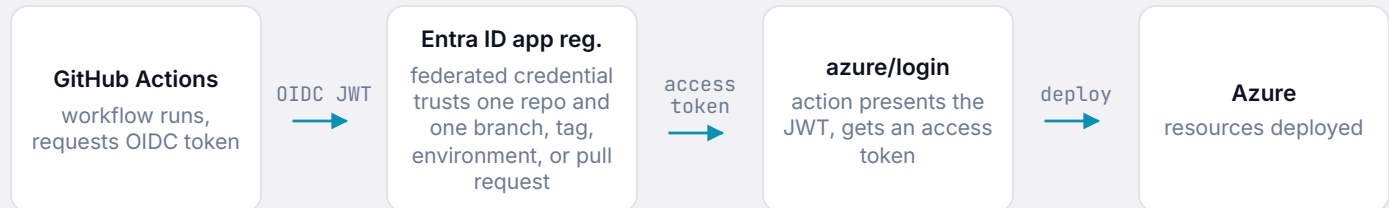
SAML 2.0 to AWS IAM Identity Center with SCIM 2.0.



SCIM is a separate connection: Entra ID provisions users and groups into IAM Identity Center, and the permission sets there decide what each of them can reach.

GitHub Actions + Azure (CI/CD authentication)

OIDC with workload identity federation. No stored secrets.



This replaces long-lived service principal secrets. The federated credential matches one repository and one branch, tag, environment, or pull request.

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

An assertion is the signed statement the IdP sends about the user. A claim is one item inside it: 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 an attacker using a stolen or injected authorization code. Required in OAuth 2.1, apart from a narrow exception for confidential clients.

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. In the AWS flow above, IAM Identity Center creates an IAM role for each permission set, and the temporary credentials for assuming it come from AWS STS.

08 These are not standards

Common terms that name an experience or a pattern rather than 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, or push. SMS counts too, and NIST restricts it: SP 800-63B-4 calls a one-time code sent over the phone network a restricted authenticator, and requires whoever issues it to offer an unrestricted alternative at the same assurance level and to tell subscribers why (section 3.2.9).

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	Enterprise customers that require it, 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 what an app may do; it does not prove who the user is. Use OIDC for login.

- **Accepting a token without checking it**

Verify the signature against the issuer's published keys, then check the issuer, the audience, and the expiry on every token. OIDC clients check the nonce as well. A library that only decodes a JWT has not validated anything. A SAML assertion needs its own checks: the signature, the audience, the recipient URL, the InResponseTo value, and the NotOnOrAfter window (SAML profiles, section 4.1.4.3).

- **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. Entra ID Conditional Access accepts one for its Multifactor, Passwordless MFA, and Phishing-resistant MFA strengths.
- Google Workspace accepts a passkey as a 2-Step Verification method, but a Context-Aware Access rule written on the MFA claim rejects one. Those rules have to check for a software key too.
- 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](#). Every enterprise IdP supports it, some procurement and compliance rules require it, and an older IdP may not offer OIDC at all. [OIDC](#) is increasingly accepted.

App needs to call Microsoft Graph or Google APIs

[OAuth 2.0](#) following [RFC 9700](#) 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, and the trust is scoped to one repository and one branch, tag, environment, or pull request.](#)

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.](#)

REF 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

ISO/IEC 26131:2024, OpenID Connect Core 1.0 · iso.org/standard/89056.html

W3C: WebAuthn Level 3 · w3.org/TR/webauthn-3/

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

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

IETF: RFC 9700, OAuth 2.0 security best practice · datatracker.ietf.org/doc/html/rfc9700

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: RFC 7642, SCIM definitions and requirements · datatracker.ietf.org/doc/html/rfc7642

IETF: RFC 7643, SCIM 2.0 core schema · datatracker.ietf.org/doc/html/rfc7643

IETF: RFC 7644, SCIM 2.0 protocol · 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

OpenID Foundation: Shared Signals Framework 1.0 · openid.net/specs/openid-sharedsignals-framework-1_0-final.html

Microsoft: authenticate apps and users with Entra ID · learn.microsoft.com/entra/architecture/authenticate-applications-and-users

Microsoft: SAML versus OpenID Connect · learn.microsoft.com/entra/identity/enterprise-apps/saml-vs-oidc-decision-guide

Microsoft: passkeys in Entra ID · learn.microsoft.com/entra/identity/authentication/concept-authentication-passkeys-fido2

Microsoft: Conditional Access authentication strengths · learn.microsoft.com/entra/identity/authentication/concept-authentication-strengths

Microsoft: continuous access evaluation · learn.microsoft.com/entra/identity/conditional-access/concept-continuous-access-evaluation

Google Workspace: SSO profiles for third-party IdPs · knowledge.workspace.google.com/admin/apps/setting-up-ssso

Google Workspace: deploy 2-Step Verification · knowledge.workspace.google.com/admin/security/deploy-2-step-verification

Google: Context-Aware Access credential strength · docs.cloud.google.com/access-context-manager/docs/custom-access-level-spec

Microsoft: KnowBe4 SSO tutorial ·

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

Microsoft: KnowBe4 provisioning tutorial ·

learn.microsoft.com/entra/identity/saas-apps/knowbe4-security-awareness-training-provisioning-tutorial

KnowBe4: SAML account settings ·

support.knowbe4.com/hc/en-us/articles/12769050560403

Udemy Business: SCIM provisioning · business-

[support.udemy.com/hc/en-us/sections/4419746964887-](https://support.udemy.com/hc/en-us/sections/4419746964887-System-for-Cross-domain-Identity-Management-SCIM-Provisioning)

[System-for-Cross-domain-Identity-Management-SCIM-Provisioning](https://support.udemy.com/hc/en-us/sections/4419746964887-System-for-Cross-domain-Identity-Management-SCIM-Provisioning)

Auth0: inbound SCIM ·

auth0.com/docs/authenticate/protocols/scim

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