# User Management (EDU-200)

**Application Programming Interface (API)** – A set of definitions and protocols for building and integrating application software.

**Internet Protocol (IP)** – A set of standards for addressing and routing data on the Internet.

**Identity Providers (IdP)** – A service that stores and verifies user identity. IdPs are typically cloud-hosted services, and they often work with single sign-on (SSO) providers to authenticate users.

**Data Protection** – Measures and practices focused on ensuring the confidentiality, integrity, and availability of data, protecting it from unauthorized access, corruption, or theft.

**JSON-based web tokens (JWT) –** An open standard that defines a compact and self-contained way for securely transmitting information between parties as a JSON object.

**Multi-Factor Authentication (MFA)** - A security process that requires users to provide more than just a password to log in to an account.

**OIDC** - OpenID Connect is an authentication protocol based on the OAuth 2.0 framework, which provides single sign on. It allows to verify a user's identity and obtain their profile information. OIDC does not store passwords, which can help prevent credential-based data breaches.

**Software-as-a-service (SaaS)** – A cloud-based software model that delivers applications to end-users through an internet browser.

**Security Assertion Markup Language (SAML)** – Security Assertion Markup Language (SAML) is an open federation standard that allows an identity provider (IdP) to authenticate users and then pass an **authentication token to another application known as a Service Provider (SP).**

**System for Cross-domain Identity Management (SCIM)** – An open standard that allows for the automation of user provisioning. SCIM makes user data more secure and simplifies the user experience by automating the user identity lifecycle management process.

**SAML just-in-time (JIT) provisioning** – A SAML protocol-based method that is used to create users the first time they log in to an application via an identity provider. This eliminates the need to provision users or create user accounts manually.



© 2026 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners. Zscaler, Inc. (HQ)

120 Holger Way
San Jose, CA 95134
+1 408.533.0288
zscaler.com

**SCIM provisioning** - A provisioning method to automate the provisioning process by providing a standard protocol to seamlessly exchange data between identity providers and cloud apps. It's widely used because it's secure and greatly reduces manual effort for IT teams.

**Service Providers (SP)** – A Service Provider (SP) is an application or service that enables users to access its resources and services using a Single Sign-On (SSO) token issued by an Identity Provider (IdP).

**Single Sign-on (SSO)** – An authentication scheme that allows users to sign in using one set of credentials to multiple independent software systems.

**User Attributes** – Information related to users, such as roles, permissions, and personal details, which systems use to enforce security policies and control access to resources.

**Extensible Markup Language (XML)** - XML is a markup language that provides rules to define any data and is used to store and transport the data.

**Zscaler Digital Experience (ZDX)** – A service built as a multi-tenant, cloud-based monitoring platform to probe, benchmark, and measure the digital experiences for every single user within your organization.

**Zscaler Internet Access (ZIA)** – A cloud native security service edge (SSE) solution that builds on a decade of secure web gateway leadership.

**ZIdentity –** A unified identity service for Zscaler that centralizes and simplifies identity management, user authentication, and entitlement assignment for users to Zscaler services.

**Zscaler Private Access (ZPA)** – A Zscaler's service that enables organizations to provide access to internal applications and services while ensuring the security of their networks.

**Zero Trust Architecture (ZTA)** – A data-centric methodology that focuses on protecting resources over the network perimeter.

**Zero Trust Exchange (ZTE)** – A cloud-native platform that allows direct and secure connections based on the principle of least-privileged access, which means that no user or application is inherently trusted. Trust is built based on the user's identity and on context, such as the user's location, the security posture of the device, the content being exchanged, and the application being requested.



© 2026 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners. Zscaler, Inc. (HQ)

120 Holger Way
San Jose, CA 95134
+1 408.533.0288
zscaler.com