User Management (EDU-200)

OAuth 2.0

OAuth 2.0 is an open standard and a security framework for delegated authorization.

It allows a third-party application (the 'Client') to obtain limited, temporary access to a user's data on another service (the 'Resource Server'), without ever exposing the user's actual login credentials (username and password) to that third-party application.

OpenID Connect (OIDC)

- OpenID Connect is an authentication protocol based on the OAuth 2.0 framework, which provides Single Sign-On (SSO). 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.
- OAuth 2.0 is the industry standard for sharing user data securely with third-party applications without exposing credentials, widely adopted in tech, social media, and finance sectors.
- OIDC empowers developers to create secure, user-friendly systems that prioritize privacy and streamlined authentication for modern applications.

SAML (Security Assertion Markup Language)

SAML (Security Assertion Markup Language) is a mature, XML-based standard favoured for enterprise, browser-based applications, while OIDC (OpenID Connect) is a modern, JSON-based, lightweight protocol built on OAuth 2.0 that excels in API-driven and mobile-first environments.

ZIdentity

ZIdentity is a centralized, unified identity and access management service designed to provide a single, secure "front door" for managing administrator roles, entitlements, and user authentication across all Zscaler products (ZIA, ZPA, etc.). It consolidates fragmented management, enabling single sign-on (SSO), enhanced multifactor authentication (MFA), and simplified user provisioning.

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

System for Cross-domain Identity Management

SCIM (System for Cross-domain Identity Management) is a standardized method for managing user identities across different systems, ensuring consistent and up-to-date information.

Understanding SCIM is essential for automating user management and ensuring seamless, consistent identity data across multiple applications. Here is a list of uses of SCIM.

- Provision users and groups into Zscaler
- Automatically update users' group or department changes
- Deprovision users when they are removed from the directory

Role-Based Access Control (RBAC)

As organizations grow, managing permissions for every individual user becomes complex and inefficient.

RBAC is an access-management method where permissions are tied to specific roles within a system. Instead of giving access to each user manually, administrators assign users to the roles that match their job responsibilities.

Not all vulnerabilities pose the same level of threat. Vulnerability management involves assessing the severity of each and prioritizing remediation based on factors like the Common Vulnerability Scoring System (CVSS) score, asset criticality, and exploitability

Monitoring

Since new vulnerabilities are discovered regularly, vulnerability management is not a one-time activity but an ongoing, iterative process

Identification

Scanning systems and networks for known vulnerabilities, such as unpatched software, misconfigurations, or outdated protocols

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

Remediation

After vulnerabilities are identified and prioritized, they are patched, mitigated, or accepted based on the risk they pose and the organization's resources.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) adds an extra layer of security by requiring users to verify their identity with two or more factors, something you know (password), something you have (device or token), or something you are (biometric).

Why MFA is Critical for Admins?

MFA is critical for administrators as it ensures secure access to critical systems, minimizes the risk of unauthorized logins, and meets compliance requirements for user authentication.

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