Protect identities and secrets

Fortify protections across every layer of the stack, from identity infrastructure to integration layers for apps and services.

99%

of employees now have video-based user verification enabled.

The Secure Future Initiative (SFI) addresses the increasing scale, speed, and sophistication of cyberattacks. Launched as a multi-year endeavor, SFI evolves how Microsoft designs, builds, tests, and operates products and services to achieve the highest possible standards for security. The six SFI pillars include goals and actions that define our approach to security.

And the **protect identities and secrets** pillar focuses on reducing credential-related risk by investing heavily in modern identity standards.

Customer guidance

Customers can strengthen their organization's security posture by **providing phishing-resistant authentication methods** and **implementing strong identity-proofing solutions** in user onboarding and recovery processes. Additionally, customers can better protect secrets and prevent them from becoming exploited by attackers by **using Azure Managed Identities** instead of client secrets for service-to-service (S2S) authentication.

Best practices include:

Phishing-resistant methods:

Employ phishing-resistant authentication methods such as certificate-basedΩ authentication, Windows Hello for Business, MacOS platform Single Sign On (SSO), FIDO2 security keys, and Microsoft Authenticator passkeys.

Implement strong identity-proofing solutions:

In user onboarding and recovery processes, using capabilities like Microsoft Entra's Temporary Access Pass.

User personas:

Determine user personas and prioritize them based on risk and complexity.

Platform readiness:

Verify that platform versions support phishing-resistant authentication.

Microsoft progress to date

Managed Identities for Azure resources is designed to replace the manual processes of managed client secrets in favor of a platform-managed identity, so secrets are not mishandled in operational processes (such as during resource setup, testing, or secret rotation).

Microsoft actions

To adopt managed identities broadly across Microsoft, we:

- **Identified** all resource types in our environments and offerings that provide and require secrets for workload authentication.
- **Generated** action items for all teams, pairing them with detailed guides for each resource type to help developers update their services.
- **Built** support for policies to prevent resources being created with client secrets.
- **Established** a clear standard across Microsoft that client authentication for these resources must move to Azure Managed Identity.
- **Tracked** adoption across the company and regularly reviewed status and obstacles with organization leaders.
- **Audited and tracked** all resources that allow traditional client secrets to enforce the standard for blocking their usage.