Microsoft Entra Engineering Connect

June 2026

Hello, June!

Welcome to the June edition of our monthly newsletter, summarizing the latest news and developments in the exciting, ever-evolving world of Microsoft Entra.

What went into General Availability (GA) since May 2026?

- Enable Phish-Resistant MFA for Linux Desktops with Microsoft Entra - Microsoft Entra extends Phish Resistant Multi-Factor Authentication support to Linux desktops through the Microsoft identity broker, closing a long-standing gap in cross-platform identity. This update brings Linux to parity with Windows and macOS, enabling secure, modern authentication using phishing-resistant credentials. Support is now available for Ubuntu 24.04 and 26.04, as well as RHEL 8, 9, and 10, helping organizations consistently enforce strong authentication across all major desktop platforms.
- Enable improved B2C-to-External ID migration with High Scale Compatibility (HSC) mode – HSC mode is a new tenant-level migration option that lets Azure AD B2C customers transition their applications to Microsoft Entra External ID without re-registering users or resetting passwords, by keeping existing B2C credentials in place during coexistence. It's intended for high-scale tenants - generally those with 5 million or more objects - where the standard bulk migration with JIT password sync isn't practical. Tenants below the 5M threshold should continue to use the standard migration path, and even eligible high-scale tenants should carefully evaluate both options before choosing. Customers can run the B2C Policy Analyzer to assess migration readiness, and account teams and partners should engage the EEID migration team to guide eligible Azure Active Directory B2C customers toward the right migration path.
- Enable system-preferred authentication for first and second factors - Microsoft Entra ID updates system-preferred authentication to apply to both first-factor and second-factor authentication in Microsoft Managed state. The system evaluates registered credentials for the user and selects the highest-ranked method for each authentication step. This update applies automatically in the Microsoft managed state, ensuring seamless and secure authentication experiences.
- Modernize account management with redesigned My Account pages - Microsoft Entra introduces redesigned **Devices, Security Info,** and **Organizations pages** in the My Account portal. The **Devices** page simplifies registered device management and prominently surfaces BitLocker recovery keys, reducing IT helpdesk dependency. The **Security Info** page in **Settings & Privacy** centralizes profile information, language, and region settings for easier updates. The **Organizations** page resolves issues with end users leaving organizations and delivers a streamlined experience. These updates automatically roll out to Microsoft Entra ID customers by the end of June 2026, requiring no administrator action.
- Cross-tenant group synchronization in Microsoft Entra - This enables organizations to synchronize security groups and memberships across tenants for centralized management and consistent access control. This simplifies cross-tenant collaboration by allowing groups managed in a source tenant to be used in one or more target tenants for scenarios like shared application access and resource authorization. Beyond collaboration, this enables more seamless cross-tenant administration by allowing organizations to extend governance and access control consistently across tenant boundaries.

- Account discovery for connected applications in Microsoft Entra ID Governance - Administrators gain visibility into all accounts within connected applications, including orphan accounts not assigned to the enterprise application in Microsoft Entra. Generate discovery reports directly from the provisioning experience to identify access gaps and simplify application onboarding. This capability requires a Microsoft Entra ID Governance or Microsoft Entra Suite license.
- Automate agent identity sponsorship transitions - Microsoft Entra ID Governance ensures agent identities always have a delegated human sponsor accountable for their access and lifecycle. With Lifecycle Workflows, when a sponsor leaves the organization, sponsorship automatically transfers to their manager, maintaining continuity. Lifecycle workflows can also notify cosponsors and managers of impending sponsorship changes, streamlining the process and reducing manual oversight.
- Drive Passkey Adoption with Microsoft Entra Registration Campaigns - Microsoft Entra Registration Campaigns now supports Passkeys such as Fast Identity Online (FIDO2), as an authentication method. Administrators can configure registration campaigns to nudge users to register passkeys during sign-in, helping organizations drive passkey adoption. This first rollout experience is optimized for users in a passkey profile without restrictions.
- App Deactivation for Microsoft Entra applications - App Deactivation introduces a safe, reversible, and self-service way for app owners and admins to turn off applications that are unused, deprecated, or under investigation - without deleting them or breaking tenant-level governance. Deactivating an app registration provides a reversible way to prevent the application from accessing protected resources without permanently removing it from your tenant. When you deactivate an application, it immediately stops receiving new access tokens, but existing tokens remain valid until they expire. This approach is useful for security investigations, temporary suspension of suspicious applications, or when you need to maintain application configuration data. Unlike permanently deleting an application, deactivation preserves all application metadata, permissions, and configuration settings, making it easy to reactivate the application if needed. The application remains visible in your tenant's enterprise applications list, but users can't sign in and no new tokens are issued.
- Enable phishing-resistant sign-in with Microsoft Entra passkeys on Windows - Users register device-bound passkeys in the local Windows Hello container and use them for secure sign-in with Windows Hello biometrics or PIN. These passkeys function as FIDO2 credentials and work without requiring the device to be Microsoft Entra joined or registered. This capability is automatically available in tenants where passkey profiles permit Windows Hello as a provider, supporting phishing-resistant authentication for Entra-protected cloud resources. Interactive Windows console sign-in is not supported.

New in Public Preview

- Support domain-less SAML Federation on workforce tenants - Domainless SAML federation with a SAML Identity Provider allows external users to authenticate into your apps or workforce resources using their IdP-managed credentials, regardless of their email domain. Domainless federation removes the need for domain matching between the user's email and pre-configured IdP domains during sign-in or invitation redemption.
- Sensitivity labels for Entra security groups - Microsoft Entra ID supports applying Microsoft Purview sensitivity labels to Entra cloud security groups in public preview. This enables administrators to use the same labels and policies already used for Microsoft 365 groups to govern security group behaviors such as guest access and other controls. Sensitivity labels are managed in Microsoft Purview and can be applied through the Entra Admin Center, Azure portal, and Microsoft Graph, helping organizations apply consistent governance across identities and access.
- Safely remove and restore devices with Device Soft Delete - This enables administrators to move device objects to a recoverable state instead of permanently deleting them. Organizations can restore devices within a defined retention period while preserving critical data like device identity and

associated security artifacts. The feature supports Microsoft Entra joined, registered, and hybrid joined devices, reducing risks from accidental deletions and improving device lifecycle management.

- Move SAP SuccessFactors Provisioning to Workload Identity-based authentication - Microsoft Entra introduces Workload Identity-based authentication for SAP SuccessFactors provisioning, replacing long-lived usernames and passwords with Entra-managed credentials and short-lived, standards-based access tokens. This update allows customers to perform this authentication upgrade in-place on their existing provisioning jobs, without recreating or restarting them. This will switch their Entra or SuccessFactors integrations to a more secure model that is aligned with SAP SuccessFactors' plan to deprecate basic authentication for SAP SuccessFactors' APIs by November 2026. The new option applies to SAP SuccessFactors inbound provisioning to Active Directory and Microsoft Entra ID, as well as writeback scenarios, and improves security by eliminating the need to manually handle credentials and rotate them periodically.
- Govern Azure role assignments with access packages - Microsoft Entra enables governance of eligible and active assignments to Azure roles at the Management Group, Subscription, and Resource Group levels through access packages. Role assignments now follow the same request, approval, and lifecycle governance model as apps and groups. This simplifies managing access to Azure resources at scale while supporting least privilege and just-in-time access principles.
- Automate user attribute updates in Lifecycle Workflows - Microsoft Entra introduces the User Attribute Updates task in Lifecycle Workflows, enabling automated attribute changes directly within workflows. Administrators can set or clear attribute values including custom attributes with a secure, consistent, and auditable process. This feature reduces manual effort, enhances governance, and scales identity automation with confidence.
- Improve privileged identity response for Security Operations Center (SOC) – Microsoft is extending the Entra Security Operator role so SOC analysts can take identity response actions such as disable users, revoke sessions, mark users compromised, force password resets (including cloud-only accounts), and delete individual authentication methods , directly from the Microsoft Defender unified role-based access control (RBAC) experience, without broad Entra admin roles or identity and access management (IAM) escalation during active incidents. Permissions are scoped to non-admin users enabling faster containment, least-privilege boundaries, and auditability.

Announcements

- Require registered methods for Self-Service Password Reset - Microsoft Entra Self-Service Password Reset (SSPR) will only accept explicitly registered authentication methods for identity verification starting September 7, 2026. Directory-sourced contact information, such as phone numbers and email addresses stored as user object properties, will no longer be accepted unless registered as authentication methods. This change applies to all users, including administrators, across Public cloud, GCC, GCC High, and DoD. Beginning July 6, 2026, Microsoft will automatically launch a registration campaign prompting affected users to register authentication methods after sign-in. Administrators should ensure users have at least one registered method to meet SSPR policy requirements before enforcement to avoid disruptions.
- Enforce conditional Access during credential registration - Starting **July 6, 2026,** Entra ID Conditional Access policies scoped to the **Register security information** user action will be evaluated during credential registration for Windows Hello for Business and macOS Platform SSO .This ensures registration policies apply consistently across all registration flows. Users must satisfy policy controls, such as multifactor authentication (MFA), network restrictions, device compliance, or other tenant defined requirement before completing registration. Organizations without Conditional Access policies targeting this user action are unaffected, and MFA remains required by default for all passwordless credential registrations. Enforcement completes by July 13, 2026.

- Expand passkey policy size and profiles in authentication methods policy - Microsoft Entra increases the passkey (Fast Identity Online 2, FIDO2) policy size limit to a dedicated 20 KB allocation within the authentication methods policy. Previously, all authentication methods shared a single 20 KB limit. This update ensures passkey policies have their own allocation, simplifying adoption and advanced targeting scenarios. Additionally, the maximum number of passkey profiles per tenant increases from 3 to 10, allowing greater flexibility in managing passkey configurations.

New guidance and information

- Global Secure Access Operations Guide - The new GSA Operations Guide is your post-deployment companion for running Global Secure Access reliably at scale. It covers alerting, health checks, change management, metrics, and recovery playbooks, with ready-to-use KQL queries and templates you can adopt on day one. Capability-specific guides are included for Private Access, Internet Access, Remote Networks, and Microsoft Traffic.

Tell us what you think!

If you have feedback on this newsletter, fill out the dedicated Microsoft Form.

Blogs

Check out the latest blog posts on our Microsoft Entra Blog and our Microsoft Entra Identity Developer Blog.

What's new in Microsoft Entra?

Learn what is new with Microsoft Entra, such as the latest release notes, known issues, bug fixes, deprecation functionality, and upcoming changes. You can find releases specific for Sovereign Clouds on a dedicated release notes page.

Become a certified Microsoft Identity and Access Administrator

Check out the certification and related training for the Microsoft Identity and Access Administrator available for customers and partners.