Microsoft Entra Engineering Connect

July 2026

July Cheers!

Welcome to the July 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 June 2026?

- Microsoft Entra Backup and Recovery - A capability that helps organizations restore a tenant after accidental or malicious changes. On by default, it automatically backs up critical directory objects, including users, groups, applications, Service Principals, managed identities, Conditional Access policies, named locations, agent IDs, and authentication and authorization policies, so admins can return to a known good state. The service takes daily backups of supported objects and retains them for 7 days with Microsoft Entra ID P1 or P2 licenses. Admins can view snapshots, compare changes, and run recovery jobs. This feature is a reliable safety net to minimize downtime and strengthen protection against misconfigurations and security incidents.
- Direct admin assignment to external users using email address - Entitlement management admins can assign external users, not in the directory, to an access package with the user's email. Users are invited into the tenant as Guest users and are governed when Microsoft Entra ID Governance is configured.
- Bring your own device (BYOD) support for the Global Secure Access Windows client using Microsoft Entra-registered devices - Enable users and partners to access corporate resources from their own devices. Administrators can assign the Private Application traffic profile to users with internal accounts, including internal guest users. This removes the previous requirement for Windows devices to be domain-joined.
- Microsoft Entra Kerberos key rotation - Improves reliability for environments by using incoming trust referral flows. The update enhances authentication resiliency during key rollover by validating referral tickets with primary and secondary Kerberos keys. This combination reduces the likelihood of authentication failures and minimizes disruption during rotation events.
- Domainless SAML federation with a SAML identity provider - Enable external users to sign in to applications or workforce resources using their Identity Provider (IdP)-managed credentials, regardless of their email domain. With no need to match user email domains with preconfigured identity provider domains, this capability simplifies onboarding and access for external users, streamlines invitation redemption, and improves flexibility for cross-organization collaboration in Microsoft Entra.

New in Public Preview

- Strengthen AI agent security with Conditional Access - Microsoft Entra Conditional Access has broader controls to secure AI agents that leverage user accounts. Administrators can target agent user accounts more precisely by including, or excluding, agents, or by using custom security attributes for dynamic grouping. Organizations can apply Conditional Access policies, based on agent risk, require compliant devices for agents running on managed endpoints, including Windows 365 for Agents, and enforce device, network, and platform-based access conditions. These enhancements extend Zero Trust protections to agent user accounts while using the familiar Conditional Access policy experience.

- Restrict AD group changes to Microsoft Entra provisioning - Designate specific Active Directory (AD) groups so all modifications are managed through the Microsoft Entra provisioning service. This capability helps maintain consistency between Microsoft Entra ID and AD by ensuring group changes are centrally controlled. Reduce configuration drift and improve alignment across identity systems.
- Generate unique aliases with custom call-outs - Use custom call-outs with Azure Logic Apps during user provisioning to perform advanced attribute transformations that meet your organization's requirements. Custom call-outs can generate values such as unique employee aliases and are supported for create events in HR inbound, SaaS outbound, and cross-tenant synchronization provisioning flows in Microsoft Entra.

Announcements

- Jailbreak/root detection in Microsoft Authenticator - This feature strengthens security by preventing Microsoft Entra credentials from being added or used on jailbroken or rooted devices. Users move to compliant devices to continue using work or school accounts in Authenticator. It is secure by default, requires no admin configuration, and applies to iOS and Android. Personal and third-party accounts are not affected.
- Starting August 2026, Microsoft Authenticator on iOS will offer an improved backup and restore experience - Users can back up account names securely by using iCloud and iCloud Keychain with end-to-end encryption. This experience includes work or school accounts, Microsoft personal accounts, and non-Microsoft accounts like Amazon or Google, also third-party time-based one-time password (TOTP). No other credentials are included in the backup. This update removes the need for a Microsoft personal account and simplifies device setup by automatically restoring account names on new iOS devices. Users manage the feature through iCloud settings

New guidance and information

- SCIM APIs available in U.S. Government Cloud - Microsoft Entra SCIM 2.0 APIs, which went into GA, in the public cloud, earlier in 2026, are available in Microsoft U.S. Government Cloud. Organizations can use standards-based SCIM operations to provision and manage users and groups in Microsoft Entra ID from external SCIM-compatible identity sources. Enable scalable identity lifecycle management, while you reduce the need for custom integrations.

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.

Microsoft