Microsoft Entra Engineering Connect

May 2026

Joyful May!

Welcome to the May 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 April 2026?

- Network content filtering by file type in Global Secure Access - Microsoft Global Secure Access supports network-based content filtering, based on file types. Administrators can monitor and control file transfers to generative AI and software-as-a-service (SaaS) applications. Organizations can define policies to block or restrict transfers of sensitive file types, such as documents, spreadsheets, and PDFs, preventing unauthorized data exfiltration across the network. This feature adds data loss prevention (DLP) on the network level.
- Prompt injection protection - AI Gateway, part of Microsoft Global Secure Access, safeguards generative AI applications, agents, and language models. The prompt injection protection capability in AI Gateway is real-time protection against malicious prompt injection attacks on enterprise generative AI apps, a top risk for large language models (LLMs). By enforcing guardrails at the network level, prompt injection protection ensures consistent security across generative AI applications, without the need for code changes.
- Global Secure Access client on iOS and iPadOS - Global Secure Access is available on iOS and iPadOS, extending secure network access to mobile Apple devices. No new agent installation is required, the client uses Microsoft Defender for Endpoint to route traffic through Global Secure Access for Microsoft 365, Microsoft Entra Internet Access, and Microsoft Entra Private Access. This enables organizations to apply consistent Zero Trust network policies across Microsoft Windows, macOS, and iOS platforms.
- Configure Global Secure Access with Cloud Firewall and remote networks for internet access - Customers can use Global Secure Access with Cloud Firewall to apply administrator-configurable filtering: source IP, destination IP, protocol, source port, destination port for internet traffic acquired from branch offices through Global Secure Access remote networks capability.
- External user access in the Global Secure Access Windows client - Enable Microsoft Private Access for external guest users and external members signing in with their home organization's Microsoft Entra ID. The client automatically detects external tenant context and allows users to seamlessly switch to the appropriate external tenant. External guest users are now billed using Monthly Active User (MAU) licensing.
- Secure branch office Microsoft Entra Internet Access with Global Secure Access remote network connectivity - Global Secure Access remote network connectivity enables secure access to full internet, including Microsoft 365, from branch offices and remote sites using Internet Protocol Security (IPsec) tunnels, without requiring Global Secure Access on end-user devices. Traffic from customer-premises equipment, such as firewalls or routers, is routed to Global Secure Access, where centralized security controls like web filtering, cloud firewall, and threat inspection are applied at the network layer. This capability extends Zero Trust protections to branch offices and unmanaged devices such as printers, servers, kiosks, Internet of Things (IoT), and bring-your-own-device (BYOD), enabling consistent policy enforcement, unified logging, and simplified operations without additional hardware.

- View approver details for access package requests in the My Access portal - Entitlement management in Microsoft Entra ID enables requestors to view approver name, email address, and their pending access package requests in the My Access portal. Streamline communication between requestors and approvers, reduce delays in access approvals. Approver information appears, by default, to members and can be controlled at the tenant and access package level.
- Enforce Conditional Access policies on Privileged Identity Management role activation - Privileged Identity Management (PIM) in Microsoft Entra ID supports configuration of reauthentication through Microsoft Entra Conditional Access policies for role activation. Administrators can require multifactor authentication (MFA) or other Conditional Access controls when a user activates a privileged role. Help ensure elevated access is protected with current authentication signals. This enhancement strengthens privileged identity security and enforces Zero Trust principles for administrative access.
- Reduce risk with Microsoft Identity Manager 2016 Service Pack 3 - Microsoft Identity Manager 2016 Service Pack 3 (MIM 2016 SP3) delivers improved stability, broader platform compatibility, and reduced operational risk for hybrid identity environments. SP3 supports Microsoft SQL Server 2022, Microsoft SharePoint Server Subscription Edition, Microsoft Exchange Server Subscription Edition, and Microsoft System Center Service Manager DW 2022. SP3 has a new deployment option for the MIM Synchronization Service using Microsoft Azure SQL Database with managed identity authentication.
- Issuer Hints streamline certificate selection in certificate-based authentication - Microsoft Entra certificate-based authentication (CBA) supports Issuer Hints to improve the sign-in experience for users with multiple certificates installed on their devices. Issuer Hints ensures the certificate picker shows trusted certificates valid for the organization, reducing confusion and minimizing sign-in errors. This enhancement improves security and usability without requiring changes to how certificates are issued or managed.
- Certificate-based authentication on iOS - Microsoft Entra CBA is available on iOS, delivering phish-resistant authentication on Apple mobile devices. Native iOS sign-ins no longer generate unnecessary password or multifactor authentication (MFA) prompts. CBA is supported as a second factor with priority (third place) in the system-preferred MFA list. Users can select another allowed MFA method, based on tenant policy, ensuring a more secure and seamless experience.
- Certificate-based authentication elevated in system-preferred MFA list on iOS - Microsoft Entra CBA is supported as a second-factor method on iOS and is compatible with single sign-on (SSO) and Primary Refresh Token (PRT). Native iOS sign-in flows reduce unnecessary password and MFA prompts, enabling an easier user experience. In addition, CBA is third in the system-preferred MFA hierarchy, ensuring stronger, phishing-resistant authentication methods are prioritized, when available.
- Certificate Authority scoping for certificate-based authentication - Microsoft Entra now supports Certificate Authority (CA) scoping for certificate-based authentication (CBA). Tenant administrators can restrict specific certificate authorities to defined user groups. This ensures authorized users authenticate using certificates issued by a particular CA, improving security and policy enforcement. Administrators can create tailored authentication policies for differing user scenarios, while they maintain a seamless sign-in experience.
- Configurable token lifetimes in Microsoft Entra ID - This feature enables administrators to customize the lifetime of access tokens, ID tokens, and Security Assertion Markup Language (SAML) tokens issued by the Microsoft Identity Platform. Create and assign token lifetime policies to applications and Service Principals. With this capability, organizations align token duration with their security and operational needs.
- Social identity provider support for native authentication in Microsoft Entra External ID - Microsoft Entra External ID supports social identity providers (IdPs) such as Apple, Facebook, Google and custom Open ID Connect (OIDC) providers through browser-delegated, web-view, authentication in native authentication. Developers can build native sign-up and sign-in experiences using software development kits (SDKs), while keeping users in the app for primary authentication. Social IdP sign-in is handled through secure web-view flows enforced by Microsoft Entra Conditional Access. This helps

organizations streamline user onboarding, meet modern security expectations, and deliver authentication experiences customers trust.

- Prefetch Workday termination data to customize account disable logic - This update to the Workday connector addresses termination processing delays affecting workers in the Asia Pacific (APAC) and Australia and New Zealand (ANZ) regions. Admins can enable the termination look-ahead setting to prefetch data and customize deprovisioning logic for accounts in Microsoft Entra ID and on-premises Active Directory.
- Track and optimize Microsoft Entra license usage in the Microsoft Entra admin center - The License Usage page in the Microsoft Entra admin center gives organizations visibility into feature usage across the tenant. Administrators can view Microsoft Entra ID P1, P2, and Suite licenses and usage metrics for key features such as Conditional Access and risk-based Conditional Access, mapped to license tiers. Usage trends over the past six months illustrate license footprint, the value derived from Microsoft Entra, and potential over-usage risks.

New in Public Preview

- Explicit Forward Proxy for Microsoft Entra Internet Access - Explicit Forward Proxy (EFP) for Internet Access enables secure web and AI gateway features in scenarios where installation of the GSA client is difficult or not possible. EFP is an effective mechanism to protect internet traffic when users use browsers to access resources from: multi-session Virtual Desktop Infrastructure (VDI), kiosks, browsers on Linux desktops, on lightly managed devices, and on bring-your-own devices with Microsoft Edge and Intune app policies.
- Account discovery for connected applications in Microsoft Entra ID Governance - Microsoft Entra ID Governance supports account discovery for connected applications. Administrators gain visibility into accounts in connected applications, including orphan accounts not assigned to the enterprise application in Microsoft Entra. Generate discovery reports from the provisioning experience and identify access gaps while simplifying application onboarding.
- Improve privileged identity response for Security Operations Centers - Microsoft is extending the Entra Security Operator role, so a Security Operations Cetner (SOC) analyst 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. These actions are done from the Microsoft Defender role-based access control (RBAC) experience, without broad Microsoft Entra admin roles, or IAM escalation during active incidents. Permissions are scoped to non-admin users and a limited set of administrative roles, enabling faster containment, least-privilege boundaries, and auditability.
- Create app-specific sign-in experiences with branding themes - Microsoft Entra introduces branding themes to create multiple, app-specific, sign-in branding experiences, instead of a limited tenant-wide configuration. This capability supports differing audiences, use cases, and application requirements.
- Federate external tenants with Microsoft Entra ID using OIDC - Microsoft Entra ID supports OIDC federation between Microsoft Entra ID workforce and Microsoft Entra External ID tenants. Users sign in to customer-facing applications with their Microsoft Entra ID workforce identities. Users authenticate with their home tenant and access Microsoft Entra External ID tenant applications. This action eliminates the need for duplicate accounts, simplifies sign-in, and enables consistent security controls across workforce and external scenarios.
- Optimize sign-in insights with $count in Microsoft Graph - Microsoft Graph supports $count in sign-in Application Programming Interface (API) requests. Customers compute record counts in their queries. Combined with Microsoft Graph query parameters such as $filter, $select, $orderby, $top, and $expand, developers return the data they need, reduce response size, and improve application performance. These query options make it easier to build efficient, scalable solutions, especially for security and identity scenarios in Microsoft Entra, by optimizing how sign-in data is queried, processed, and presented.

Announcements

- In April 2026, Microsoft transitions from Microsoft Entra Connect Sync to the cloud-native Microsoft Entra Cloud Sync to simplify hybrid identity management and strengthen Zero Trust security. This move reduces on-premises complexity while it improves reliability, security, and day-to-day operations. Starting July 2026, customers will be notified of their assigned transition window through the Microsoft 365 Message Center, Microsoft Entra Connect Health, and targeted emails. Phased transitions start with tenants supported by Microsoft Entra Cloud Sync, and expand as capabilities grow. During the transition window, tools and guidance help you assess readiness, migrate, and test. Microsoft Entra Cloud Sync becomes the primary identity synchronization solution, with unchanged hybrid authentication experiences.
- Microsoft Entra transitions SCIM apps from OAuth authorization code grant – Microsoft Entra transitions System for Cross-domain Identity Management (SCIM) provisioning applications, from the OAuth 2.0 Authorization Code grant, to modern authentication methods: OAuth 2.0 client credentials or workload identity federation. As the service change rolls out, updated applications prompt customers to reconfigure provisioning jobs and use more secure options. Some applications, which can't migrate, will be retired from the Microsoft Entra app gallery.

  This change improves security, simplifies credential management and rotation, and prepares customers for a more resilient provisioning experience. Customers are advised to not create new provisioning jobs using the Authorization Code grant and instead to monitor upcoming What's New updates for timelines and guidance from the Microsoft Entra team.

New guidance and information

- New video | Build secure verification with Microsoft Entra Verified ID - Ever wonder what secure, seamless identity verification looks like? In this video, see the full journey with Microsoft Entra Verified ID. From an organization issuing digital credentials, to individuals presenting and verifying them. Whether you're looking for a quick deployment or a tailor-made solution, Microsoft Entra Verified ID flexes to fit your identity verification requirements.
- Microsoft Entra ID Governance guest usage monitoring workbook - Administrators can monitor and understand guest user governance activity under the new Monthly Active User (MAU) billing model for Microsoft Entra ID Governance. The workbook has billable governance actions, so admins can track guest usage, forecast costs, and optimize governance posture before billing enforcement. It's located under Identity Governance and Access in Microsoft Entra ID Workbooks.
- Troubleshoot prompt injection protection article - This article walks through prompt injection protection policies that help Global Secure Access administrators inspect, and control malicious prompts sent to AI services and reduce the risk of sensitive data exfiltration. It provides steps to validate that policies are applying as expected.

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.