Microsoft

Security in the new Outlook for Windows

February 4, 2025

As the intended replacement for Outlook for Windows (classic), the new Outlook for Windows will soon be renamed to “Outlook for Windows”. For clarity, this document refers to the new Outlook for Windows as ”new Outlook” to differentiate from the ”Outlook for Windows (classic)”, or “classic Outlook”.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.

Introduction

This whitepaper provides a security overview of the new Outlook for Windows, providing details on the application architecture, security features, and how organizations can secure, manage, and govern email and related data. The new Outlook incorporates modern security standards, protocols, and defaults, ensuring robust protection against evolving threats. It also adheres to the Microsoft Security Development Lifecycle (SDL), a comprehensive security assurance process that informs every stage of design, development, and deployment.

The new Outlook for Windows and Outlook on the web share the same code base, integrating with Microsoft Windows through native APIs.

Key security features include:

- Client support for all Exchange Online security features including anti-malware / spam / phishing, Conditional access, and DLP.

- Built-in and supported robust security features and customizable options such as S/MIME, DLP, and modern authentication controls.

- Continuous improvement of security controls and monitoring to meet current and future threats.

Governance

This section outlines the governance framework for the new Outlook, known as the Microsoft Regulatory Governance Program. The program provides implementation guidance and oversight over the engineering process to comply with Security, Privacy, Regulatory Compliance, Responsible AI (RAI) and Digital Safety requirements.

Each feature and capability built in the new Outlook is reviewed for adherence to Microsoft standards. Detailed threat models are created to track data movement across data boundaries, and privacy reviews are conducted to ensure the product is adhering to data classification standards. RAI reviews are conducted to respect data boundaries and to uphold Microsoft values. Let’s briefly review each area.

Security. Security is a top priority in designing any Microsoft product. The new Outlook follows the Microsoft Security Development Lifecycle (SDL), a comprehensive process that ensures security during design, development, and deployment. This includes design requirements, attack surface analysis, and threat modeling to predict and mitigate vulnerabilities and threats throughout the product's lifecycle.

Privacy. Microsoft believes that Privacy is a fundamental human right. As part of our responsibility to defend this right, we keep Privacy at the center of how we shape the products and services that customers use every day. We ground our privacy commitments in strong data governance practices that must be upheld by every employee.

As with classic Outlook, the new Outlook adheres to the Microsoft Privacy Standard. Features and capabilities that access and store customer data are reviewed by privacy managers for compliance to Microsoft privacy policies.

Regulatory Compliance. The new Outlook follows Microsoft regulatory compliance implementation guides to meet country- and governmental-specific requirements such as GDPR and EUDP, and in reporting on service incidents and availability.

Responsible AI (RAI)

RAI at Microsoft is about cutting-edge research, top engineering systems, high standards in policies, and excellence in corporate processes. Microsoft has AI principles guiding the development and deployment of AI technologies, including Copilot. These principles focus on fairness, reliability and safety, privacy and security, inclusiveness, transparency, and accountability.

The new Outlook's AI must meet specific requirements to mitigate potential harms and uphold Microsoft values:

- **Impact Assessments**: Document known harms and planned mitigations to identify and address potential risks before deployment. These assessments are reviewed by multiple entities to ensure Responsible AI commitments are met and high-priority harms are avoided.
- **Red-Teaming and Incident Response**: Test the AI system to surface potential harm and inform necessary mitigations. Incident response mechanisms track and address AI incidents.

- **Continuous Evaluation**: Regularly measure and evaluate AI outputs to ensure they meet responsible AI standards.

By integrating these practices, Copilot and AI in the new Outlook aims to provide a secure and ethical user experience.

Data Security

The new Outlook uses existing, well-tested and hardened protocols to communicate with services via the common codebase with Outlook on the web. The new Outlook for Windows interacts with Exchange Online servers to handle emails, calendar events, and other daily tasks. The client and service work together to enforce strong security measures, including Conditional Access policies from Entra ID.

New Outlook provides best in class integration of email protection (anti-spam, malware, phishing) and compliance with full client support (e.g. blocked + allowed senders) and visibility into client actions for eDiscovery and auditing.

To further secure messaging, the new Outlook for Windows includes robust and customizable security features such as S/MIME, DLP, and authentication controls. These protections are enabled by default and continuously improved to address current and future threats.

The new Outlook with Copilot is designed with security and responsible AI principles at its core:

- **Data Protection:** Adheres to Microsoft's security, governance, compliance, and privacy policies, ensuring data stays within the Microsoft 365 Service Boundary.
- **Permission Management:** Respects existing permissions and policies, ensuring sensitive data is only accessible to authorized individuals.
- **Risk-Based Conditional Access:** Organizations can use risk-based conditional access and endpoint management to block or restrict risky access.

Application architecture

The new Outlook is designed for agility, built on the web codebase (Outlook web client). Architecturally, it is an extensive wrapper around the web experience designed to integrate and leverage publicly available OS capabilities for performance, storage and deep integration with platform specific features like notifications. It uses a hybrid app model with a Win32 native host that embeds a WebView2 object for the UX/UI layer and hosts other Win32 native modules, combining the reach of web apps with the power of native apps. The web UI is projected into the native app using WebView2, which allows for local data and synchronization. By default, the new Outlook for Windows uses the most stable version of Microsoft Edge and the WebView2 runtime.

Key Security Benefits of WebView2:

- Accelerates innovation, deployment, and bug fixes by standardizing technology between the email client and the browser.

- Ensures users are on the most current builds.
- Helps manage releases and maintain compliance.

Secure Communications:

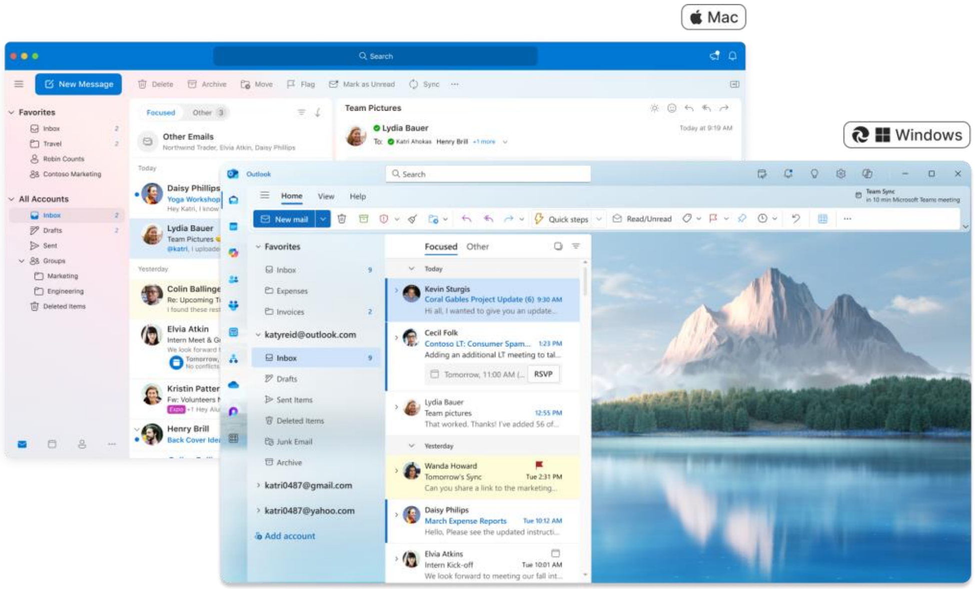
- Files and logs are stored under specific directories in the local file system like classic Outlook for Windows.

Unique Application ID:

- The new Outlook uses a unique application ID to isolate security risks, provide granular access control and reduce the risk of unauthorized access. This approach also improves monitoring, auditing, and compliance as the new Outlook application ID is not used by other workloads.

Web code base:

A foundational benefit of the new Outlook is to provide a common user experience across large screen clients, while leveraging the capabilities and interaction model of the underlying platform.



Using the same codebase as the Outlook web client allows for simultaneous delivery of features across both clients through the M365 service-based flighting infrastructure.

Key Functional Differences

Considerable effort has been made to maintain consistency in terms of capabilities between Outlook Web and the new Outlook client whenever possible. Differences generally come from platform capabilities and limitations including:

- **Windows UI integration.** The most obvious visual difference between the clients is where new Outlook leverages OS native UI and behavior including native windowing controls, removal of the browser bar / controls, and removal of the Office navigation waffle.
- **Multi-account support**. The new Outlook allows users to add more than one account into the Folder list such as an account from a different tenant, 3rd party email providers (including IMAP / POP), a PST file, or shared mailbox. Outlook web currently has limited multi-account support (focused on archive, shared, and delegate mailbox access).
- **Windows OS integration.** As a native application, the new Outlook has access to Windows OS APIs that are otherwise unavailable to web apps. These include seamless integration with other Win32 apps like the Teams and Office apps, access to local files including Office's MRU, and standard OS elements like notifications, protocol and file handlers.
- **S/MIME.** Relative to Outlook web, S/MIME in the new Outlook client leverages the Crypto APIs available on the OS. This simplifies the overall architecture for the feature and enables access to a broader range of encryption algorithms as well as enabling some advanced features that were previously only available on classic Outlook.
- **Offline capabilities**. As a native application, the new Outlook has the ability for persistent storage, resulting in significantly more offline capabilities relative to Outlook web. This currently includes offline access to emails and calendar with limited ability to access attachments and create emails / calendar events (more coming soon).
- **PST support.** A specific implementation of local file access, rich PST support like classic Outlook is only possible from a native application and the capabilities afforded by local storage.

Release process

The new Outlook follows the M365 release process, introducing features and fixes through service-based flighting instead of build updates. Almost all client-web changes are controlled by a feature flight, and updates are applied automatically to keep users current, secure, and stable without requiring admin actions.

Client web version, Webvew2 version, new Outlook version and deployment are provided in Settings > General > About Outlook.

- **Feature Rollouts:** The release process for the new Outlook follows the same path as web, using several internal validation rings to monitor feature performance and make the worldwide release as robust as possible. Features listed on the Microsoft 365 Roadmap* are released into the Targeted Release ring for 30 days before becoming generally available in General Availability (Standard Release). Large customers are advised to have some users in Targeted Release to

preview features and prepare their organization.
*Some Copilot features may go directly to General Availability release.

- **Issue Resolution:** If issues arise, organizations can raise a support ticket during the Targeted Release month. Microsoft will disable the feature for their tenant while the issue is resolved. For long-term issues, an admin setting will be released to disable the feature during the Targeted Release window.
- **Targeted Release:** Organizations are encouraged to add some or all their users to Targeted Release to get new features as soon as they start rolling out to production. Targeted Release is a fully supported production ring.
- **Rollout Monitoring:** Microsoft feature teams may choose to roll out more slowly or target specific user groups first. Rollouts are closely monitored for adverse impacts, and rollbacks are possible at all stages.

Authentication Protocol Support

This section discusses the use of web-based protocols in the new Outlook. Web-based protocols are more compatible with cloud services and third-party applications, which is important as organizations move towards hybrid and multi-cloud environments. These protocols, such as OAuth and OpenID Connect, offer several benefits over older methods such as NTLM and Kerberos. They are more scalable and flexible, working across different platforms and devices. They also include advanced security features like token-based authentication, which can reduce the risk of replay attacks.

Policy management

This section details methods used to administer policy controls for the new Outlook. The new Outlook can be managed using Conditional Access policies, Office Cloud Services policies, and OwaMailbox policies. This policy approach allows tenant admins to control user behaviors and data access, ensuring robust data security, user interaction management, and application configuration.

Key controls include the ability to separate business and personal communications to prevent data leakage and appropriately handle sensitive data. Policies can be configured to manage security features such as email encryption/decryption and control the visibility of sensitive information like user details and group memberships.

OwaMailboxPolicy policies: Sharing its client codebase with web, admins can manage the new Outlook using the same Powershell cmdlets like Set-OwaMailboxPolicy, Set-CASMailbox and Set-OrganizationConfig, providing a consistent policy management experience across the two clients. Additionally, there are a few specific policies for the new Outlook for features specific to the native client such as multi-account and offline. Admins can enable or disable personal accounts and specify allowed organization account domains.

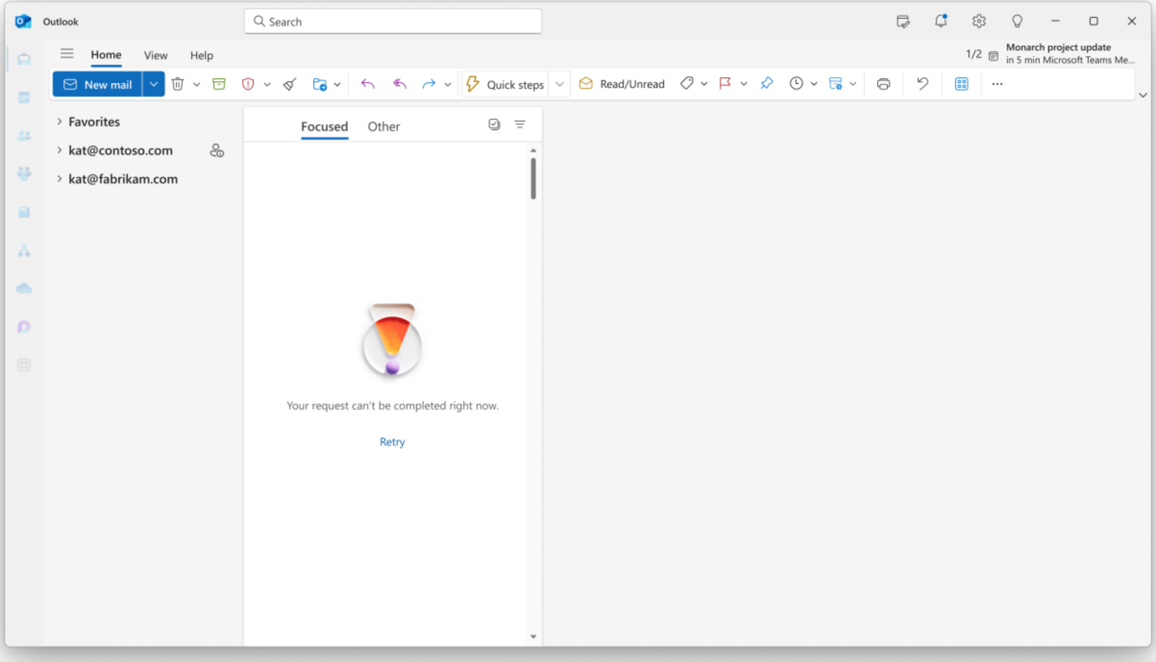
The policy Set-CASMailbox OWAEnabled will block the use of both OWA and the new Outlook. However, work is underway to decouple this policy so that tenants can block either Outlook web or new Outlook, both, or neither.

Detailed policy management capabilities for the new Outlook can be found here.

Conditional Access (CA) policies. CA policies generate claims that are embedded in access tokens. These claims are assessed when accessing resources, such as to prevent access from unmanaged devices. Like Outlook web and classic Outlook, resources accessed by Outlook perform validation of relevant claims.

Continuous Access Evaluation (CAE). CAE is a Conditional Access policy that is uniquely evaluated. CAE provides a quick response to policy violations or security issues. For example, if a user's location requires more verification, they might need to confirm with their phone. If there's a password breach, the organization can force an immediate password change for all users.

Like web and classic Outlook, the new Outlook uses CAE to subscribe to critical Microsoft Entra ID events. CAE enforces policies in real-time. For instance, IP addresses are validated on every request, and any pre-issued tokens are checked for validity if an admin revokes access. On a claim challenge, the new Outlook continues to work for all accounts except the one with the issue. The claim-challenged account will remain inaccessible until the user fulfills the claim requirements with EntraID.

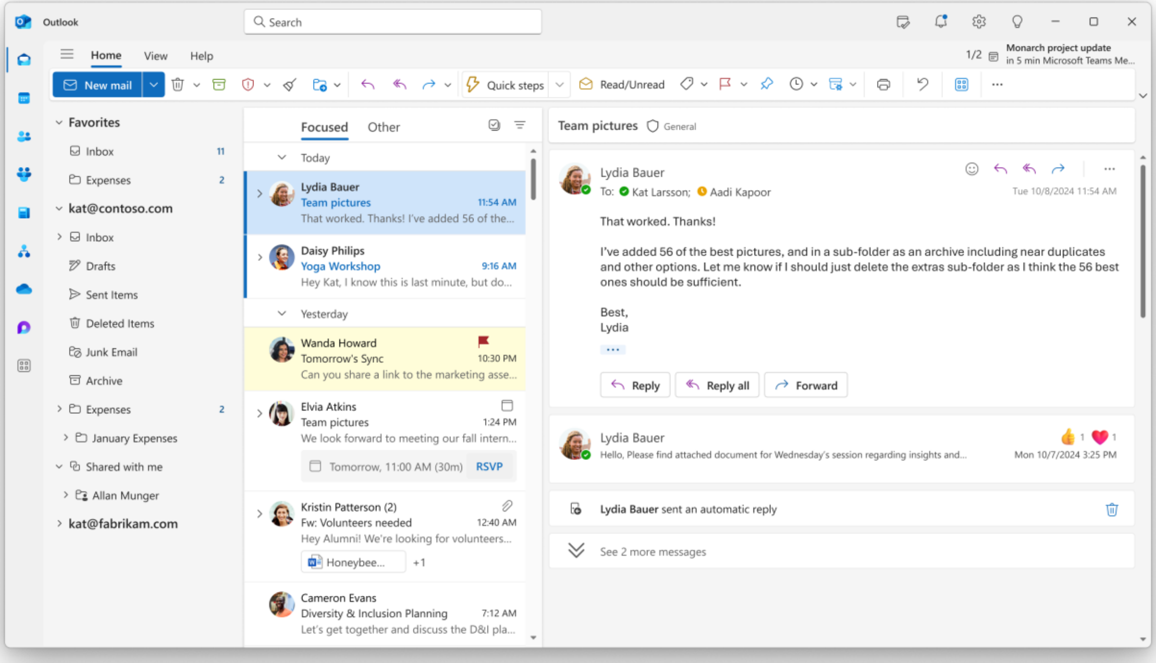


Your request can't be completed right now.

Accounts

This section describes the way in which accounts are added, configured and remediated in the new Outlook. The new Outlook is a multi-account client, supporting the ability to add multiple email accounts so users can manage all their mailboxes in one place. The new Outlook supports 1st party email accounts (Microsoft EntraID and Microsoft accounts such as outlook.com, hotmail.com) and 3rd party accounts (e.g. Gmail, Yahoo, iCloud, IMAP and POP accounts). EntraID accounts can also access additional mailboxes, like shared or delegated ones.

Each email account added to the new Outlook is active and syncing in the background.



Lydia Bauer
Team pictures 11:54 AM
That worked. Thanks! I've added 56 of the...

Daisy Philips
Yoga Workshop 9:16 AM
Hey Kat, I know this is last minute, but do...

Wanda Howard
Tomorrow's Sync 10:30 PM
Can you share a link to the marketing asse...

Elvia Atkins
Team pictures 1:24 PM
We look forward to meeting our fall intern...
Tomorrow, 11:00 AM (30m) RSVP

Kristin Patterson (2)
Fw: Volunteers needed 12:40 AM
Hey Alumni! We're looking for volunteers...
Honeybee... +1

Cameron Evans
Diversity & Inclusion Planning 7:12 AM
Let's get together and discuss the D&I pla...

Team pictures General

Lydia Bauer
To: Kat Larsson; Aadi Kapoor
Tue 10/8/2024 11:54 AM

That worked. Thanks!

I've added 56 of the best pictures, and in a sub-folder as an archive including near duplicates and other options. Let me know if I should just delete the extras sub-folder as I think the 56 best ones should be sufficient.

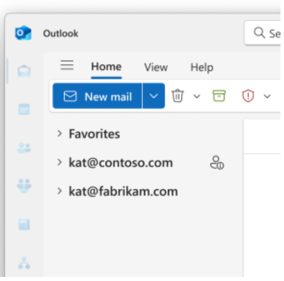
Best,
Lydia

Lydia Bauer
Hello, Please find attached document for Wednesday's session regarding insights and...
Mon 10/7/2024 3:25 PM

Lydia Bauer sent an automatic reply

See 2 more messages

Account remediation. Accounts that face authentication, authorization, or policy issues are marked as needing attention. Users must select the account to start the remediation process. Once the issue is resolved, the email account will become accessible.



Account settings. The new Outlook has two types of settings: global settings and account settings.

- **Global settings** apply across all email accounts in the application. These include settings like dark mode, conversation mode, and Calendar view. They stay the same no matter which account the user is using.
- **Account settings** are specific to each email account. These include autoreplies and signatures. They can cause different actions for different mailboxes, like showing notifications for work emails but not personal ones. When you switch email accounts, the account settings change accordingly.

Global settings are applied from the Primary email account. The Primary email account is the first account added and can later be changed in Settings > email accounts. It stores privacy settings and opt-ins for connected services and diagnostic data. Organizations can control the Primary account via OCS policies.

Account policies. Some organizations require the ability to limit configured accounts to those for a specific tenant while others may need to allow different tenancies. In many cases, it is also permissible to allow personal accounts to be set up alongside work or school accounts. The new Outlook can support these configurations using the following OwaMailbox policies:

`-PersonalAccountsEnabled`

`-AllowedOrganizationAccountDomains`

The following policy in the Cloud Policy service for Microsoft 365 is used to configure the Primary account to ensure it is used during application boot in a pre-authentication state:

`Require the Primary Account to match the Windows signed-in account`

OWAMailbox policies are documented here.

Authentication

This section explains how the new Outlook handles authentication. It supports the latest security features like Conditional Access, Continuous Access Evaluation, and Proof of Possession. The new Outlook can authenticate both Microsoft and 3rd-party email accounts, as well as shared mailboxes and licensing accounts.

For Microsoft EntraID and Microsoft accounts, it uses OneAuth-MSAL, which is Microsoft's standard identity platform. This platform uses OAuth2 to authenticate users. For EntraID accounts, Token protection, also known as PoP, validates that tokens are only used on the intended device, providing strong security against token theft.

For 3rd-party accounts, Microsoft’s Mailbox Replication Service (MRS) syncs the user's mail from 3rd-party services to Exchange Online. For Google and Yahoo, the new Outlook uses OAuth2. For iCloud, IMAP, and POP accounts, Basic Auth is used to add the accounts, but OAuth2 is used for ongoing communication. MRS handles token refresh activities for all 3rd-party accounts, ensuring continuous interaction with various internal services. Tokens are securely stored and are refreshed as needed.

Resiliency

This section outlines authentication resiliency support in the new Outlook. The application uses Microsoft’s EntraID backup authentication system to keep things running smoothly during EntraID service interruptions. This backup system works separately from EntraID and kicks in automatically when needed. It helps reduce the impact of any authentication service failures.

The EntraID backup authentication service helps applications to authenticate users even if EntraID is having problems by using session data to provide seamless authentication during outages.

S/MIME

This section explains Secure/Multipurpose Internet Mail Extensions (S/MIME) support in the new Outlook. S/MIME helps protect sensitive information by allowing users to send signed and encrypted emails within their organization. Administrators can enable S/MIME-based security if they have mailboxes in Exchange Online. S/MIME provides end-to-end encryption and digital signatures, ensuring email content remains confidential and the sender's identity is verified.

Emails are encrypted before leaving the user’s device, and only the intended recipient can decrypt and read them. Digital signatures verify the sender's identity, and the email content hasn't been tampered with during transit. There are three types of S/MIME messages: encrypted, signed, or both signed and encrypted.

Unlike Outlook for the web, the new Outlook's S/MIME support doesn't require installing a separate component or browser extension. S/MIME DLLs are already part of new Outlook setup and are invisible to the user.

Use OWAMailbox policies for S/MIME as described here S/MIME for message signing and encryption | Microsoft Learn.

Data Loss Prevention

This section explains how the new Outlook supports Microsoft Purview Data Loss Prevention. Data Loss Prevention (DLP) helps identify, monitor, and protect sensitive data. For example, DLP can detect social security or credit card numbers in an email and alert users before they send it.

Administrators can customize restrictions, such as warning users about sensitive data, requiring authorization, or blocking the data from being sent. The new Outlook supports several DLP features to enhance security and compliance.

- **Sensitivity labels with or without encryption:** Admins can create policies for auto labeling, mandatory labeling, and default labeling. Labels are applied via the Sensitivity button.
- **Conditions and actions**: Transport rules, also known as mail flow rules, are a key component of how Data Loss Prevention (DLP) policies work in Outlook and Exchange. Admins can use Transport Rules to act on sensitivity labels.

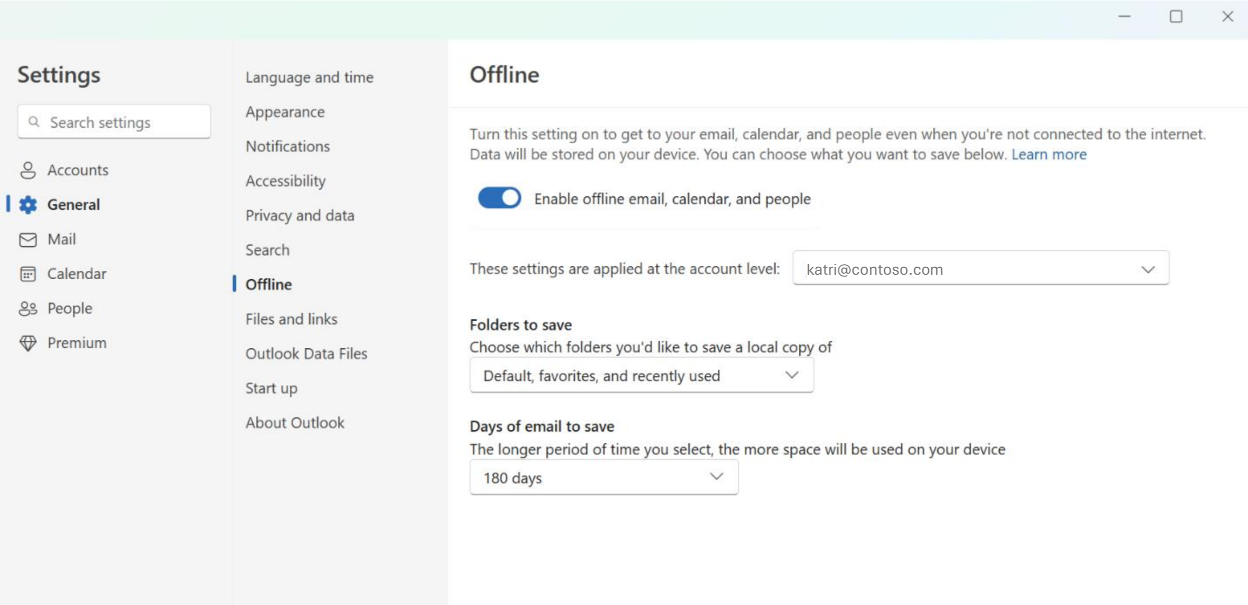
- **Rights management/IRM Templates**: Provides online and offline protection for emails and attachments, preventing unauthorized printing, forwarding, or copying.
- **Prevent Copilot summarization**: Sensitivity labels that are configured for rights management can prevent Copilot from accessing sensitive content, as well as blocking copying and screen captures.
- **DLP Policy Tips**: Notifies users when they attempt to send sensitive information that violates DLP policies.
- **Oversharing Pop-up**: Alerts users when they are about to share sensitive information.
- **Highest sensitivity**: Admins can set label policy to match the highest sensitivity label from attachments. This is not currently supported (Microsoft 365 Roadmap Feature ID: 117579)

With these features, the new Outlook can provide robust security and compliance capabilities like the classic Outlook for Windows.

Offline

This section explains how offline support works in the new Outlook. Instead of using OST files like the classic Outlook, the new Outlook uses a sync engine that runs on a web worker to download data and save it locally in an IndexedDB database. This allows users to access their data offline. The data is stored in %localappdata%\Microsoft\Olk\EBWebView\Default\IndexedDB and can be encrypted with Windows BitLocker.

You can configure the amount of data saved offline in Settings > General > Offline. If you want to disable offline capabilities, you can use the OfflineEnabledWin parameter in the Set-OwaMailboxPolicy Exchange PowerShell cmdlet. Setting this parameter to $false will prevent any items from being saved to the device, making the app online-only, like Outlook web.



Offline

Turn this setting on to get to your email, calendar, and people even when you're not connected to the internet. Data will be stored on your device. You can choose what you want to save below. Learn more

● Enable offline email, calendar, and people

These settings are applied at the account level: katri@contoso.com

Folders to save
Choose which folders you'd like to save a local copy of
Default, favorites, and recently used

Days of email to save
The longer period of time you select, the more space will be used on your device
180 days

Web Add-ins

This section explains the security benefits of web add-ins in the new Outlook compared to COM add-ins. The new Outlook, similar to Outlook on the web and Microsoft Teams, exclusively supports web add-ins, which provide several security benefits:

- **Sandboxing**: Web add-ins run in a separate environment, reducing the risk of crashes and compatibility issues.
- **Modern security practices**: They use secure messaging and well-defined interfaces for data exchange, ensuring data is securely formatted and transmitted.
- **Faster updates**: Updates can be deployed simultaneously across platforms, accelerating innovation and bug fixes.
- **Stricter certification**: Only Microsoft 365 Certified add-ins are shown in the Store, ensuring higher security standards.

Overall, web add-ins provide a more stable, secure, and efficient experience.

Conclusion

In conclusion, the new Outlook for Windows offers robust built-in security features that simplify data protection. It provides administrators with the flexibility to configure, manage, and integrate security measures tailored to their business needs. This delivers a secure and efficient email experience for users.

Helpful links

- **WebView2:** Microsoft Edge WebView2 | Microsoft Edge Developer
- **MSAL:** Overview of the Microsoft Authentication Library (MSAL) - Microsoft identity platform | Microsoft Learn.
- **Policy management:** Policy Management - Microsoft 365 Apps | Microsoft Learn
- **OWAMailbox policies:** Set-OwaMailboxPolicy (ExchangePowerShell) | Microsoft Learn.