What's new in Microsoft Intune

Summarize this article for me

Learn what's new each week in Microsoft Intune.

You can also read:

- **Important notices**
- Past releases in the What's new archive
- Information about how Intune service updates are released

ⓘ **Note**

Each **monthly update** can take up to three days to roll out and is in the following order:

- Day 1: Asia Pacific (APAC)
- Day 2: Europe, Middle East, Africa (EMEA)
- Day 3: North America
- Day 4+: Intune for Government

Some features roll out over several weeks and might not be available to all customers in the first week.

For a list of upcoming Intune feature releases, see **In development for Microsoft Intune**.

For new information about Windows Autopilot solutions, see:

- **Windows Autopilot device preparation: What's new**
- **Windows Autopilot: What's new**

You can use RSS to be notified when this page is updated. For more information, see How to use the docs.

Week of January 12, 2026

App management

PowerShell script installer for Win32 apps

When adding a Win32 app, you can upload a PowerShell script to serve as the installer instead of specifying a command line. Intune packages the script with the app content and runs it in the same context as the app installer, enabling richer setup workflows like prerequisite checks, configuration changes, and post-install actions. Installation results appear in the Intune admin center based on the script's return code.

For more information, see Win32 app management in Microsoft Intune.

Applies to:

- ✓ Windows

Week of December 8, 2025

Device enrollment

ACME protocol support for iOS/iPadOS and macOS enrollment

As we prepare to support managed device attestation in Intune, we are starting a phased rollout of an infrastructure change for new enrollments that includes support for the *Automated Certificate Management Environment (ACME) protocol*. Now when new Apple devices enroll, the management profile from Intune receives an ACME certificate instead of a SCEP certificate. ACME provides better protection than SCEP against unauthorized certificate issuance through robust validation mechanisms and automated processes, which helps reduce errors in certificate management.

Existing OS and hardware eligible devices do not get the ACME certificate unless they re-enroll. There is no change to the end user's enrollment experience, and no changes to the Microsoft Intune admin center. This change only impacts enrollment certificates and has no impact on any device configuration policies.

ACME is supported for Apple Device Enrollment (BYOD), Apple Configurator enrollment, and automated device enrollment (ADE) methods. Eligible OS versions include:

- iOS 16.0 or later
- iPadOS 16.1 or later
- macOS 13.1 or later

New Setup Assistant screens now generally available for iOS/iPadOS and macOS automated device enrollment profiles

You can hide or show 12 new Setup Assistant screens during automated device enrollment (ADE). The default is to show these screens in Setup Assistant.

The screens you can skip during iOS/iPadOS enrollment, and the applicable versions, include:

- **App Store** (iOS/iPadOS 14.3+)
- **Camera button** (iOS/iPadOS 18+)
- **Web content filtering** (iOS/iPadOS 18.2+)
- **Safety and handling** (iOS/iPadOS 18.4+)
- **Multitasking** (iOS/iPadOS 26+)
- **OS Showcase** (iOS/iPadOS 26+)

The screens you can skip during macOS enrollment include:

- **App Store** (macOS 11.1+)
- **Get Started** (macOS 15+)
- **Software update** (macOS 15.4+)
- **Additional privacy settings** (macOS 26+)
- **OS Showcase** (macOS 26.1+)
- **Update completed** (macOS 26.1+)

- **Get Started** (macOS 15+)

For more information about available Setup Assistant skipkeys, see:

- Set up automated device enrollment for iOS/iPadOS
- Set up automated device enrollment for macOS

Week of December 1, 2025

App management

Secure enterprise browser managed by Intune (public preview)

Microsoft Intune now supports policy management for Microsoft Edge for Business as a secure enterprise browser. By implementing policies through Intune, admins can confidently transition from Windows-based desktop environments to secure, browser-based workflows for accessing corporate resources without requiring device enrollment.

For more information, see Secure Your Corporate Data in Intune with Microsoft Edge for Business.

Week of November 17, 2025

Device enrollment

Configure Windows Backup for Organizations

Windows Backup for Organizations is generally available in Microsoft Intune. With this feature, you can back up your organization's Windows settings and restore them on a Microsoft Entra joined device. Backup settings are configurable in the Microsoft Intune admin center settings catalog, while a tenant-wide setting that lets you restore a device is available in the admin center under **Enrollment**. For more information about this feature, see Windows Backup for Organizations in Microsoft Intune.

Device management

Security Copilot in Intune agents are available for public preview

Security Copilot agents in Intune are AI-powered assistants that specialize in specific scenarios. The Intune agents are available in the Intune admin center > **Agents**, and are available for Security Copilot users.

The following Intune agents are available:

- The **Change Review Agent** evaluates Multi Admin Approval requests for Windows PowerShell scripts on Windows devices. It provides risk-based recommendations and contextual insights to help admins understand script behavior and associated risks.

  These insights can help Intune admins make informed decisions more quickly about whether to approve or deny requests. This agent supports Intune-managed devices running Windows.

- The **Device Offboarding Agent** identifies stale or misaligned devices across Intune and Microsoft Entra ID. It provides actionable insights and requires admin approval before offboarding any devices. This agent complements existing Intune automation by showing insights and handling ambiguous cases where automated cleanup isn't enough.

  The agent supports Intune-managed devices running Windows, iOS/iPadOS, macOS, Android, and Linux. During public preview, admins can directly disable Microsoft Entra ID objects, with additional remediation steps provided as guidance.

- The **Policy Configuration Agent** analyzes uploaded documents or industry benchmarks and automatically identifies matching Intune settings. Admins can upload their requirements, like compliance standards or internal policy documents, and the agent intelligently shows relevant settings from the Intune settings catalog.

  The agent also guides you through policy creation and helps you configure each setting that best suits your organization's needs. This agent supports devices running Windows.

To learn more, see:

- Security Copilot agents in Intune

Intune support for iVerify as a mobile threat defense partner

You can now use iVerify Enterprise as a mobile threat defense partner (MTD) for enrolled devices that run the following platforms:

- Android 9.0 and later
- iOS/iPadOS 15.0 and later

To learn more about this support, see Set up iVerify Mobile Threat Defense Connector.

Tenant administration

Manage tasks and requests from the centralized Admin tasks node in Microsoft Intune (public preview)

The new **Admin tasks** node in the Intune admin center provides a centralized view to discover, organize, and act on security tasks and user elevation requests. Located under **Tenant Administration**, this unified experience supports search, filtering, and sorting to help you focus on what needs attention—without navigating across multiple nodes.

The following task types are supported:

- Endpoint Privilege Management file elevation requests
- Microsoft Defender security tasks
- Multi Admin Approval requests

Intune only shows tasks you have permission to manage. When you select a task, Intune opens the same interface and workflow you'd use if managing the task from its original location. This ensures a consistent experience whether you're working from the admin tasks node or directly within the source capability.

For more information, see Admin tasks.

Week of November 10, 2025 (Service release 2511)

Microsoft Intune Suite

Scope tag enforcement for Endpoint Privilege Management elevation requests

When viewing Endpoint Privilege Management elevation requests, applicable scope tags are now enforced. This means administrators can view and manage only the requests for devices and users that fall within their assigned scope. This change helps maintain administrative boundaries and strengthen security. Previously, admins with permissions to manage elevation requests could view all elevation requests, regardless of scope.

App management

More volume options available in Managed Home Screen

Admins can now enable more volume controls in the Managed Home Screen (MHS) app for Android Enterprise dedicated and fully managed devices. In addition to the existing media volume control, this update introduces configuration settings to show or hide sliders for **call**, **ring and notification**, and **alarm** volumes.

Each new option can be independently enabled through app configuration policies. When turned on, users can adjust these specific volume levels directly from the Managed Settings page within MHS, without leaving kiosk mode. This enhancement provides task workers greater flexibility to manage sound levels for different environments while keeping the device securely locked down.

For more information, see Configure the Microsoft Managed Home Screen app for Android Enterprise.

Applies to:

- ✓ Android Enterprise (dedicated and fully managed devices)

Reset Managed Google Play store mode to Basic

You can now reset the Managed Google Play store layout from **Custom** back to **Basic** in the Intune admin center (**Apps** > **All apps** > **Create Managed Google Play app**).

In **Basic** mode, all approved apps are automatically visible to users. In **Custom** mode, newly approved apps must be manually added to collections before they appear in the store. The new **Reset to Basic** button lets admins quickly revert to Basic mode without needing to contact support. When selected, Intune deletes all existing collections and immediately displays a success or failure message.

For more information about Managed Google Play store layout options, see Approve and deploy Android Enterprise apps in Intune.

Applies to:

- ✓ Android

Updated Service Level Objectives for Enterprise App Management

Service Level Objectives (SLOs) are now available in Enterprise App Management (EAM) to provide clearer expectations for when app updates become available in the Enterprise App Catalog. SLO processing timelines begin when Intune first receives the updated app package.

Most app updates complete automated validation within 24 hours. Updates that require manual vendor testing or approval typically complete within seven days.

For more information, see Enterprise App Management overview.

New cut, copy, and paste options for Windows app protection

Intune adds two new values to the **Allow cut, copy and paste for** setting in Windows app protection policies (starting with Microsoft Edge) to give admins more control over data movement:

- Org data destinations and any source: Users can paste from any source into the org context, and can cut/copy only to org destinations.
- Org data destinations and org data sources: Users can cut/copy/paste only within the org context.

These options extend familiar mobile APP data-transfer controls to Windows, helping prevent data leaks on unmanaged devices while preserving productivity. For more information, see App protection policies overview.

Applies to:

✓ Windows

Device configuration

Settings available in both Templates and Settings Catalog for Android Enterprise

Some settings that were only available in Templates are now also supported in the settings catalog.

The settings catalog lists all the settings you can configure in a device policy, and all in one place. For more information about configuring settings catalog profiles in Intune, see Create a policy using settings catalog.

To create a new settings catalog policy, go to **Devices** > **Manage devices** > **Configuration** > **Create** > **New policy** > **Android Enterprise** for platform > **Settings catalog** for profile type.

The following settings are available in the settings catalog:

General:

- Block Contact sharing via Bluetooth (work profile level)
- Block searching of work contacts and displaying work contact caller-id in personal profile
- Data sharing between work and personal profiles
- Skip first use hints

Work profile password:

- Number of days until password expires
- Number of passwords required before user can reuse a password
- Number of sign-in failures before wiping device
- Required password type
  - Minimum password length
  - Number of characters required
  - Number of lowercase characters required
  - Number of non-letter characters required
  - Number of numeric characters required
  - Number of symbol characters required
  - Number of uppercase characters required
- Required unlock frequency

To learn more about these settings, go to Android Intune settings catalog settings list.

Applies to:

- Android Enterprise

New Assist Content Sharing setting in the Android Enterprise settings catalog

The Settings Catalog lists all the settings you can configure in a device policy, and all in one place. For more information about configuring Settings Catalog profiles in Intune, see Create a policy using settings catalog.

There are new settings (**Devices** > **Manage devices** > **Configuration** > **Create** > **New policy** > **Android Enterprise** for platform > **Settings catalog** for profile type):

- **Block assist content sharing with privileged apps**: If **True**, this setting blocks assist content, like screenshots and app details, from being sent to a privileged app, like an assistant app. The setting can be used to block the **Circle to Search** AI feature.

For some guidance on managing AI features on Android devices, see Manage AI on Android with Intune - A Guide for IT Admins.

Applies to:

- Android Enterprise corporate-owned devices with a work profile (COPE) > Work profile level
- Android Enterprise corporate owned fully managed (COBO)
- Android Enterprise corporate owned dedicated devices (COSU)

Device enrollment

New opt-in upgrade allows existing customers to move from managed Google Play accounts to Microsoft Entra ID accounts

Microsoft Intune offers a new opt-in upgrade that allows existing Android Enterprise customers to move from using managed Google Play accounts to using Microsoft Entra ID accounts for Android device management. You are eligible for upgrade if you previously used a consumer Gmail account. This change streamlines the onboarding process by eliminating the need for a separate Gmail account and by leveraging your work account. This change is not required. To learn more about this change, see:

- New onboarding flow to managing Android Enterprise devices with Microsoft Intune
- Connect your Intune account to your managed Google Play account

Incomplete user enrollment report removed

The incomplete user enrollments report has been removed and is no longer functional in the Microsoft Intune admin center. The following corresponding APIs have also been removed from Microsoft Intune:

- getEnrollmentAbandonmentDetailsReport

- getEnrollmentAbandonmentSummaryReport
- getEnrollmentFailureDetailsReport

Scripts or automation using these Graph APIs will stop working now that the report has been removed. In place of this report, we recommend using the enrollment failures report. For more information, see View enrollment reports.

Device management

Query and results improvements to Explorer feature with Security Copilot in Intune

With your Security Copilot license, you can query your Intune data using the **Explorer in Intune** feature.

When you create your queries, you have more filter options. For example:

- Queries with a number operator let you choose equal, greater than, and less than values.
- Queries that forced you to choose one option, like platform, allow you to select multiple options.

In the query results, there are also more columns available to view your data.

To learn more about this feature, see Explore Intune data with natural language and take action.

Device Management Type assignment filter property supports Android enrollment options for Managed Devices

When you create a policy in Intune, you can use assignment filters to assign a policy based on rules you create. You can create a rule using different properties, like `deviceManagementType`.

For managed devices, the Device Management Type property supports the following Android enrollment options:

- Corporate-owned dedicated devices with Entra ID Shared mode
- Corporate-owned dedicated devices without Entra ID Shared mode
- Corporate-owned with work profile
- Corporate-owned fully managed
- Personally-owned device with a work profile
- AOSP user-associated devices
- AOSP userless devices

To learn more about assignment filters and the properties you can currently use, see:

- Use filters when assigning your apps, policies, and profiles in Microsoft Intune
- App and device properties, operators, and rule editing when creating filters in Microsoft Intune

Applies to:

- Android

New prompts available to explore your Intune data

You can use Security Copilot in Intune to explore new prompts related to your data using natural language. Use these new prompts to view data on:

- Users and groups
- Role based access control (RBAC)
- Audit logs

When you start typing your request, a list of prompts that best match your request are shown. You can also continue typing for more suggestions.

Each query returns a Copilot summary to help you understand the results and offers suggestions. With this information, you can also:

- Add devices or users from the results to a group so you can target apps and policies to this group.
- Filter example queries to find or build requests that match your needs.

To learn more, see Explore Intune data with natural language and take action.

Device security

Microsoft Tunnel access by rooted Android devices is blocked by the Microsoft Defender client

Microsoft Tunnel uses the Microsoft Defender client app to provide Android devices access to tunnel. The latest version of the Defender for Endpoint client can now detect when a device is rooted. If a device is determined to be rooted, Defender:

- Marks the device's risk category as *High*
- Immediately drops active Tunnel connections
- Prevents further use of Tunnel until the device is determined to no longer be rooted
- Sends a notification to the device user about the device status

This capability is a feature of the Defender client on Android and doesn't replace the use of Intune compliance policies for Android to manage the settings like *Rooted devices*, *Play Integrity Verdict*, and *Require the device to be at or under the Device Threat Level*.

For more information about features of Microsoft Tunnel, see Overview of Microsoft Tunnel.

Tenant administration

Soft-deleted Microsoft Entra groups now visible in Intune

This feature is in public preview. For more information, see Public preview in Microsoft Intune.

Microsoft Intune now displays soft-deleted Microsoft Entra groups in the Intune admin center. When a group is soft-deleted, its assignments no longer apply. However, if the group is restored, its previous assignments are automatically reinstated.

For more information, see Include and exclude app assignments in Microsoft Intune.

Week of October 20, 2025 (Service release

2510)

Microsoft Intune Suite

Support for user account context in Endpoint Privilege Management Elevation Rules

Endpoint Privilege Management (EPM) has a new option for elevation rules that runs the elevated file using the user's context instead of a virtual account. The option is **Elevate as current user**.

With the *Elevate as current user* elevation type, files or processes that are elevated run under the signed-in user's own account, rather than a virtual account. This preserves the user's profile paths, environment variables, and personalized settings, helping to ensure that installers and tools that rely on the active user profile function correctly. Because the elevated process maintains the same user identity before and after elevation, audit trails remain consistent and accurate. Prior to elevation, the user is required to enter their credentials for Windows Authentication. This process supports multifactor authentication (MFA) for enhanced security.

For more information, see Use Endpoint Privilege Management with Microsoft Intune.

Endpoint Privilege Management Dashboard for user readiness and elevation trends

You can now use an Endpoint Privilege Management (EPM) dashboard that presents insights about file elevations and trends in your organization and help identify users that might be ready to be moved to run as standard users in place of running with local admin permissions.

Insights provided by the dashboard include:

- Users who have only unmanaged file elevations
- Users who have both managed and unmanaged file elevations
- User with only managed elevations

- Frequently unmanaged elevations
- Frequently approved by support
- Frequently denied elevations

For more information about the dashboard and these new insights, see Overview dashboard in Reports for Endpoint Privilege Management.

Device configuration

System Info property available in properties catalog for device inventory

You can create a properties catalog policy that lets you collect and view hardware properties from your managed Windows devices. There's a **System Info** category that shows system-level device insights, like OS version, hardware details, and configuration state.

To learn more and get started, see properties catalog.

Applies to:

✓ Windows

New settings available in the Android Enterprise settings catalog

There are new settings in the Android settings catalog. To create a new settings catalog policy and see these settings in the Intune admin center, go to **Devices** > **Manage devices** > **Configuration** > **Create** > **New policy** > **Android Enterprise** for platform > **Settings catalog** for profile type.

- **Wi-Fi Direct**
  - **General** > **Block Wi-Fi Direct**: If **True**, this setting blocks Wi-Fi Direct. Wi-Fi Direct is a direct, peer-to-peer connection between devices using Wi-Fi frequencies. If **False**, Intune doesn't change or update this setting. By default, the OS might allow Wi-Fi Direct.

Applies to:

- ✓ Android Enterprise corporate-owned devices with a work profile (COPE)
- ✓ Android Enterprise corporate owned fully managed (COBO)
- ✓ Android Enterprise corporate owned dedicated devices (COSU)

- **Hide organization name**

  The **General** > **Hide organization name** setting supports corporate owned single use dedicated devices. Previously, this setting was only supported on corporate-owned devices with a work profile and corporate owned fully managed devices.

- Some settings that were only available in Templates are available in the settings catalog.

  General:
  - Allow copy and paste between work and personal profiles
  - Allow network escape hatch
  - Allow USB storage
  - Block access to status bar
  - Block date and time changes
  - Block location
  - Block microphone adjustment
  - Block mounting of external media
  - Block notification windows
  - Block screen capture (work profile-level)
  - Block Wi-Fi setting changes

To learn more about these settings, see Android Intune settings catalog settings list.

The settings catalog lists all the settings you can configure in a device policy, and all in one place. For more information about configuring settings catalog profiles in Intune, see Create a policy using settings catalog.

Applies to:

- ✓ Android Enterprise

Device enrollment

Edit managed Google Play organization name

Now you can edit the managed Google Play organization name directly in the Microsoft Intune admin center under **Devices** > **Android** > **Enrollment** > **Managed Google Play**. The updated name, which is validated on input, appears in the admin center. It might also appear on Android device lock screens within a message like, *This device is managed by [organization name]*. For more information, see Connect Intune account to managed Google Play account.

Device management

Settings catalog supports Windows 11 25H2 settings

The release of Windows 11 25H2 includes new policy configuration service providers (CSPs). These settings are available in the settings catalog for you to configure.

To learn more, see the Microsoft Intune Settings Catalog Updated to Support New Windows 11, version 25H2 Settings blog post.

To get started with the settings catalog, see:

- Use the Intune settings catalog to configure settings
- Common tasks you can complete using the settings catalog

Applies to:

✓ Windows

New client version for Remote Help for macOS

With the new Remote Help client, version 1.0.2510071, Microsoft Intune now supports macOS 26. Earlier versions of the Remote Help client aren't compatible with macOS 26. The app is automatically updated through Microsoft AutoUpdate (MAU) if opted-in, so no action is required from you or your users. The latest client version resolves an issue that previously caused the screen to appear blank on first launch and fail to connect. For more information, see Use Remote Help with Microsoft Intune.

Device security

Intune to end support for legacy Apple MDM software updates

With the release of iOS 26, iPadOS 26, and macOS 26, Apple has deprecated legacy mobile device management (MDM) software update commands and payloads. To align with this change, Intune will soon end support for the following MDM-based workloads:

- iOS/iPadOS update policies
- macOS update policies
- Software update settings in:
  - iOS/iPadOS **templates** > **Device restrictions**
  - iOS/iPadOS **settings catalog** > **Restrictions**
  - macOS **templates** > **Device restrictions**
  - macOS **settings catalog** > **Restrictions**
  - macOS **settings catalog** > **Software update**
- Reports:
  - iOS/iPadOS update installation failures
  - macOS update installation failures
  - macOS per-device software updates

These functionalities are now available through declarative device management (DDM), which provides a more modern and reliable approach to managing Apple software updates. For more information about this transition, see the Intune Customer Success blog Move to declarative device management for Apple software updates .

Applies to:

✓ iOS/iPadOS
✓ macOS

Intune apps

Newly available protected apps for Intune

The following protected apps are now available for Microsoft Intune:

- Total Triage by CareXM
- Intapp by Intapp Inc.
- ANDPAD by ANDPAD Inc.
- ANDPAD CHAT by ANDPAD Inc.
- ANDPAD Inspection by ANDPAD Inc.
- ANDPAD Blueprint by ANDPAD Inc.

For more information about protected apps, see Microsoft Intune protected apps.

Monitor and troubleshoot

Enrollment time grouping failure report generally available for Android and Windows

Now generally available in the Microsoft Intune admin center, the enrollment time grouping failures report shows failures, which include devices that failed to become a member of the specified static device group during one of the following processes:

- Windows Autopilot device preparation provisioning
- Enrollment of Android Enterprise fully managed devices
- Enrollment of Android corporate-owned work profile devices
- Enrollment of Android Enterprise dedicated devices

The enrollment time grouping failures report is available in the admin center under **Devices** > **Monitor** > **Enrollment time grouping failures**. Recently updated information could take up to 20 minutes to appear in the report. For more information, see Enrollment time grouping in Microsoft Intune.

Week of October 13, 2025

Device management

Windows 10 support in Intune

On October 14, 2025, Windows 10 reached end of support and won't receive quality and feature updates. Windows 10 is an **allowed** version in Intune. Devices running this version can still enroll in Intune and use eligible features, but functionality won't be guaranteed and can vary.

For more information, see Support statement for Windows 10 in Intune.

Applies to:

- ✓ Windows 10

Week of September 29, 2025

App management

PowerShell script installer support for Enterprise App Catalog apps

You can now upload a PowerShell script to install Enterprise App Catalog apps as an alternative to using a command line. This option gives you more flexibility when deploying apps.

For more information, see Add an Enterprise App Catalog app to Microsoft Intune.

Applies to:

- ✓ Windows

End of support for older versions of the Android Intune Company Portal app

Support for Android Intune Company Portal versions earlier than **5.0.5421.0** ended on October 1, 2025. Devices running an older version of the app might no longer maintain their registration status and can be marked noncompliant.

To keep devices registered and compliant, users must download the latest version of the Company Portal from the Google Play Store .

Applies to:

- ✓ Android Enterprise

Week of September 22, 2025

Device security

Update for the Vulnerability Remediation Agent for Security Copilot in Intune (public preview)

We've updated the Vulnerability Remediation Agent for Security Copilot, adding the following changes to the ongoing limited public preview:

- **Role-based access control (RBAC) for Microsoft Defender** - We've updated the RBAC guidance to reflect how RBAC is implemented in Microsoft Defender XDR. Guidance is now provided for configurations that use **Unified RBAC** (a single set of permissions across services) and for **granular RBAC** (customized permissions per service).

  When using granular RBAC configurations, ensure the agent's identity is scoped in Microsoft Defender to include all relevant device groups. The agent can't access or report on devices outside its assigned scope.

- **Agent Identity** – You can now manually change the account that the agent uses as its identity. From the agents *Settings* tab, select **Choose another identity** to open a sign-in prompt. Enter and authenticate the new account. Ensure the new account has sufficient permission to access the Microsoft Defender Vulnerability Remediation data.

  Changes to the agent's identity won't affect the agent's run history, which remains available.

These updates provide greater flexibility and control for organizations using the Vulnerability Remediation Agent in preview. To learn more about this Agent, see

Vulnerability Remediation Agent for Security Copilot in Microsoft Intune.

Week of September 15, 2025 (Service release 2509)

Device configuration

Filter device configuration profiles by the policy type

In the Intune admin center > **Devices** > **Configuration** > **Policies** tab, you can use the **Add filters** feature to filter your list of policies by platform, scope tags, and the last modified date.

Policy type is available in the **Add filters** feature. So, you can filter your list of policies by their type, like the settings catalog, custom, device restrictions, and the other policy types.

To learn more about viewing and monitoring existing profiles, see View and monitor device configuration policies in Microsoft Intune.

New day zero settings available in the Apple settings catalog

The Settings Catalog lists all the settings you can configure in a device policy, and all in one place. For more information about configuring Settings Catalog profiles in Intune, see Create a policy using settings catalog.

There are new settings in the Settings Catalog. To see these settings, in the Microsoft Intune admin center, go to **Devices** > **Manage devices** > **Configuration** > **Create** > **New policy** > **iOS/iPadOS** or **macOS** for platform > **Settings catalog** for profile type.

iOS/iPadOS

Managed Settings > **Default Applications:**

- Calling
- Messaging

Restrictions:

- Allowed Camera Restriction Bundle IDs

Web > **Web Content Filter**:

- Safari History Retention Enabled

macOS

Authentication > **Extensible Single Sign On Kerberos**:

- Use Platform SSO TGT

Microsoft Defender:

- The Microsoft Defender category is updated with new settings. Learn more about available macOS Defender settings at Microsoft Defender - Policies.

Restrictions:

- Allow Call Recording
- Allow Live Voicemail

Web > **Web Content Filter**:

- Safari History Retention Enabled

Settings available in both Templates and Settings Catalog for Android Enterprise

Some settings that were only available in Templates are now also supported in the settings catalog.

The settings catalog lists all the settings you can configure in a device policy, and all in one place. For more information about configuring settings catalog profiles in Intune, see Create a policy using settings catalog.

To create a new settings catalog policy, go to **Devices** > **Manage devices** > **Configuration** > **Create** > **New policy** > **Android Enterprise** for platform > **Settings catalog** for profile type.

The following settings are in the settings catalog:

Applications:

- Allow installation from unknown sources
- App auto-updates (work profile-level)

General:

- Block roaming data services
- Block Bluetooth configuration
- Block Wi-Fi access point configuration
- Default permission policy
- Block access to camera
- Allow access to developer settings
- Block beaming data from apps using NFC (work-profile level)

  This setting is deprecated in A10. While it still configures correctly on newer devices, it has no effect because the feature isn't available.

- Block factory reset
- Block tethering and access to hotspots
- Block volume changes

  This setting appears as successfully applied to corporate-owned devices with a work profile, but it has no effect.

System Security:

- Require threat scan on apps
- Require Common Criteria mode

Users and accounts:

- User can configure credentials (work profile-level)
- Block account changes

To learn more about these settings, see Android Intune settings catalog settings list.

Applies to:

✓ Android Enterprise

Device management

Device category management supports Multi Admin Approval

Intune device categories support Multi Admin Approval. When Multi Admin Approval is enabled, changes to device categories, including creating a new one, editing or deleting one, require a second administrator to approve the change before it's applied. This dual authorization process helps protect your organization from unauthorized or accidental role-based access control changes.

For more information on multiple administrative approval, see Use multiple administrative approvals in Intune.

New Private Space and USB access settings in the Android Enterprise settings catalog

The Settings Catalog lists all the settings you can configure in a device policy, and all in one place. For more information about configuring Settings Catalog profiles in Intune, see Create a policy using settings catalog.

There are new settings (**Devices** > **Manage devices** > **Configuration** > **Create** > **New policy** > **Android Enterprise** for platform > **Settings catalog** for profile type):

- **Block private space**: When set to **True**, users are prevented from creating or using private spaces on the device. All existing private spaces are deleted.

Applies to:
✓ Android Enterprise corporate-owned devices with a work profile (COPE)

- **USB access**: Allows admins to select what files and/or data can be transferred via USB. If admins block file transfer, only files are blocked from being transferred. Other connections are allowed, like a mouse. If admins block USB data transfer, all data is blocked.

  Applies to:
  ✓ Android Enterprise corporate-owned devices with a work profile (COPE) (At work profile level)
  ✓ Android Enterprise corporate owned fully managed (COBO)
  ✓ Android Enterprise corporate owned dedicated devices (COSU)

For a list of existing settings you can configure in the settings catalog, see Android Enterprise device settings list in the Intune settings catalog.

New prompts available to explore your Intune data

You can use Microsoft Copilot in Intune to explore new prompts related to your Intune data using natural language. Use these new prompts to view data on:

- Android and Apple device updates
- Windows Autopilot
- Endpoint Privilege Management
- Advanced Analytics

When you start typing your request, a list of prompts that best match your request are shown. You can also continue typing for more suggestions.

Each query returns a Copilot summary to help you understand the results and offers suggestions. With this information, you can also:

- Add devices or users from the results to a group so you can target apps and policies to this group.
- Filter example queries to find or build requests that match your needs.

To learn more, see Explore Intune data with natural language and take action.

Intel vPro Fleet Services integration in Intune partner portal

Microsoft Intune now integrates with Intel vPro Fleet Services, bringing hardware-level remote management directly into the Intune experience. This solution enables IT admins to securely manage, recover, and troubleshoot Intel vPro devices even when the operating system is unresponsive, or the device is powered off. With Microsoft Entra ID single sign-on, teams gain authenticated access without requiring more infrastructure or licensing.

Key capabilities include:

- Hardware-level BIOS and OS recovery through Intel Active Management Technology (AMT)
- Centralized workflows within Intune
- Enhanced security and access control
- Broad compatibility with Intel vPro devices (2018 or later)

This integration simplifies endpoint management and improves operational efficiency, and scales to support diverse device fleets.

Device Inventory (formerly Resource explorer)

The **Resource explorer** pane under **Monitor** for Windows devices is now called **Device Inventory**. Only the name changed—the experience and data remain the same.

References in Intune documentation and the Intune admin center are updated to reflect the new name.

Applies to:

✓ Windows

> ⓘ **Note**
>
> The **Resource explorer** pane that displays Configuration Manager data via tenant attach still retains its original name.

New features in Copilot for Microsoft Intune

- **Easier access to Copilot Chat** - Copilot Chat is embedded directly into the Intune admin center header. So, IT admins can access Copilot Chat from any screen in the admin center. This feature helps admins get faster insights and support.

- **Context-aware conversations with Copilot Chat** - As you type, a dynamic prompt box provides real-time suggestions and recommends prompts relevant to what you're trying to ask. You can troubleshoot devices, manage policies, explore Windows 365 features, and more. You can also directly access the Microsoft docs to learn more.

  Copilot Chat retains your conversation history and remains context aware as you move through the admin center. This continuity helps minimize repetitive prompts.

- **Expanded support for Windows 365 Cloud PC** - With this general availability update, Copilot now supports Windows 365 Cloud PC management. IT admins can access important info, like licensing status, connection quality, configuration details, and performance metrics. This feature makes it easier for admins to monitor and manage Cloud PCs directly from the Intune admin center.

To learn more about Copilot in Intune and to get started, see Microsoft Copilot in Intune.

Intune supports iOS/iPadOS 17.x as the minimum version

Apple released iOS 26 and iPadOS 26. With this release, Microsoft Intune—including the Intune Company Portal and app protection policies (APP, also known as MAM)—now requires iOS/iPadOS 17 or later.

For more information on this change, see Plan for change: Intune is moving to support iOS/iPadOS 17 and later.

> ⓘ **Note**
>
> Userless iOS and iPadOS devices enrolled through Automated Device Enrollment (ADE) have a slightly nuanced support statement due to their shared usage. For more information, see Support statement for supported versus allowed iOS/iPadOS versions for user-less devices .

Applies to:

✓ iOS/iPadOS

Intune supports macOS 14.x as the minimum version

Apple released macOS 26 (Tahoe). With this release, Microsoft Intune, the Company Portal app, and the Intune MDM agent now require macOS 14 (Sonoma) or later.

For more information on this change, see Plan for change: Intune is moving to support macOS 14 and later.

> ⓘ **Note**
>
> macOS devices enrolled through Automated Device Enrollment (ADE) have a slightly nuanced support statement due to their shared usage. For more information, see Support statement .

For a list of supported OS version, see Supported operating systems and browsers in Intune.

Applies to:

✓ macOS

Device security

New security baseline update experience

The Intune security baseline update experience is updated for the more recent versions of security baselines. With this change, when you update a security baseline that was created after May 2023 to a more recent version of that same baseline, you now have two options to help automatically configure the updated baseline:

- Keep customizations – With this option, Intune applies all the settings customizations from the original baseline that you're upgrading to the new baselines template. The result is that the new baseline instance retains (includes) all your organization's specific modifications.
- Discard customizations – With this option, Intune creates a new 'default' baseline

instance that uses the new baseline version. Each setting in that baseline uses the baseline default and none of your settings customizations are automatically applied.

With both options, your decision is applied to a new profile instance of that baseline, which uses the latest baseline version. This new profile won't have the scope tags or assignments from the original, which you can add later after the new profile has been created. This change gives you time to configure other settings if desired before the updated profile is assigned and begins to deploy the latest baseline version to devices. Meanwhile, your original baseline is left unchanged and remains active. But, its setting configurations become read-only.

For more information, see Update a baseline profile to the latest version in Manage security baseline profiles in Microsoft Intune.

Company Portal supports Purebred's new derived credentials experience

Apple released iOS 26 and iPadOS 26. With this update, Purebred (version 3) introduces a new and improved derived credentials experience. As part of day zero support, Company Portal supports Purebred's updated workflow.

- If your organization plans to continue using the older version of Purebred, there are no changes to your derived credentials experience in Purebred or Company Portal—even if you upgrade to the latest version of Company Portal.
- If your organization plans to upgrade to the new version of Purebred, make sure to update to Company Portal version 5.2509.0 to ensure compatibility.

Applies to:

✓ iOS/iPadOS

Monitor and troubleshoot

Give feedback about multiple device query

Use the new feedback feature on the multiple device query page to submit feedback about multiple device query.

Week of September 8, 2025

Device security

JavaScript WebSockets support with Microsoft Tunnel for Mobile Application Management for iOS

Microsoft Tunnel for Mobile Application Management (MAM) for iOS now supports JavaScript WebSockets from web views. This support helps improve communications for apps that require real-time communications that rely on WebSockets.

While JavaScript WebSockets are now supported, Tunnel for MAM iOS doesn't support native WebSocket APIs or apps that rely on them.

For more information, see Microsoft Tunnel for Mobile Application Management for iOS/iPadOS admin guide.

Week of September 1, 2025

Device management

Enrollment Status Page support for installing Windows security updates during Windows OOBE

> ⓘ **Important**
>
> Beginning on January 13, 2026, this capability is available. The first Windows Update that is offered as available is the `2026–01 B` quality update.

The Windows out-of-box experience (OOBE) by default installs the latest available security updates to help ensure devices are secure and up to date from day one. Windows OOBE is used by Intune and by Windows Autopilot scenarios through the Intune enrollment status page (ESP) configurations. Intune refers to these security updates Windows quality updates.

To help you manage this behavior, we've updated the Intune enrollment status page with a new setting you can use to allow or block the automatic installation of these updates.

The new setting is **Install Windows quality updates**. These security updates, also known as Windows quality updates in Intune, are installed by default during the Windows out-of-box experience OOBE that's used by Intune and by Windows Autopilot.

By default, this setting is set to *Yes* in all new ESP profiles you create, which results in the most recent security updates being installed. In all your previously created ESP profiles, this setting is set to *No* until you choose to edit those profiles to change it. When set to *No*, OOBE doesn't install the updates, which can give your internal teams time to test the updates before allowing them to install on new devices you provision.

For more information about the Intune enrollment status page, see Set up Enrollment Status Page. For information about Windows quality updates, see Windows quality update policy.

Applies to:

✓ Windows

Device security

Device configuration recommendations from the Security Copilot Vulnerability Remediation Intune agent

To help reduce your organization's attack surface against vulnerabilities, the Security Copilot Vulnerability Remediation Intune agent now provides recommended configurations for settings related to a reported vulnerability.

You can find the recommended configurations after selecting *Agent suggestions* for a reported vulnerability, which opens the *Suggested action* pane. On the suggested action pane, there's a new section of information titled **Configurations**.

If the Intune settings catalog contains relevant settings for the reported vulnerability, the Configurations section provides information to help you configure device policies. These policies can help minimize future risk from that vulnerability, including:

- A list of the settings that are relevant to the current vulnerability, which can be deployed through an Intune settings catalog policy. Only the specific settings that are relevant to the vulnerability are listed.
- Each setting is presented with a recommended configuration.
- Selecting the citation icon next to a setting displays that settings description. The description can also include a link to content for the Configuration Service Provider (CSP) that the setting represents.

If there are no recommended device configuration settings to deploy, the Configurations section indicates that no recommended settings catalog policy configurations are available.

To learn more about Agent suggestions, remediation guidance, and the new recommended configurations, see Agent suggestions in *Use the Vulnerability Remediation Agent*.

Week of August 25, 2025

App management

Offline Mode and App access without sign in for Android Enterprise Dedicated Devices on Managed Home Screen

Managed Home Screen (MHS) for Android Enterprise dedicated devices now supports two new features: **Offline mode** and **App access without sign in**.

- **Offline mode** – Lets users access designated apps when the device is offline or unable to connect to the network. You can configure a grace period before requiring users to sign in once connectivity is restored.
- **App access without sign in** – Lets users launch specific apps from the MHS sign-in screen via the MHS top bar, regardless of network status. This feature is useful for apps that need to be available immediately, such as help desk or emergency tools.

These features are designed for dedicated devices enrolled in Microsoft Entra shared device mode and can be configured via device configuration policy.

Applies to:

- ✓ Android Enterprise dedicated devices

Week of August 18, 2025 (Service release 2508)

App management

Android app configuration policies support new variable values

Android Enterprise app configuration policies in Intune now support more variable values. The new values include account name, device name, employee ID, MEID, serial number, and the last four digits of the serial number.

For more information, see Supported variables for configuration values.

Applies to:

- ✓ Android Enterprise

Device configuration

Managed Installer support for user and device groups

Our Managed Installer policy is updated to add the capability to target individual groups of users and devices, using one or more individual policies. Until now, a Managed Installer policy was a tenant-wide configuration that applied to all Windows devices. With this update, separate policies can now be assigned to different device groups providing you with more flexibility.

If you previously had a tenant-wide managed installer policy in effect, that policy remains available with a group assignment to all your devices. This reconfiguration is equivalent to the previous tenant-wide configuration it had before. You can choose to use that converted policy or implement new policies with more granular control.

For more information about configuring and using managed installers, see Get started with managed installers.

Applies to:

✓ Windows

New Windows settings in the settings catalog

The Intune settings catalog lists all the settings you can configure, and all in one place. There are new settings in the Windows settings catalog (**Devices** > **Manage devices** > **Configuration** > **Create** > **New policy** > **Windows 10 and later** for platform > **Settings catalog** for profile type).

Microsoft Edge Administrative Templates policy updates:

- **v138** - Intune supports the following new ADMX-backed policies:

Expand table

Setting	CSP
Microsoft Edge > **Allow pages to use the built-in AI APIs**	BuiltInAIAPIsEnabled
Microsoft Edge > **Control access to AI-enhanced search in History**	EdgeHistoryAISearchEnabled
Microsoft Edge - Default Settings (users can override)\ Identity and sign-in > **Use Primary Work Profile as default to open external links**	EdgeOpenExternalLinksWithPrimaryWorkProfileEnabled
Microsoft Edge > **Allow SpeculationRules prefetch for ServiceWorker-controlled URLs**	PrefetchWithServiceWorkerEnabled

Microsoft Edge > **Control whether TLS 1.3 Early Data is enabled in Microsoft Edge**	TLS13EarlyDataEnabled
Microsoft Edge > **Allow pages to use the built-in AI APIs**	BuiltInAIAPIsEnabled

The following legacy settings are deprecated, and shouldn't be used:

Expand table

Setting	CSP
Microsoft Edge\ Private Network Request Settings	InsecurePrivateNetworkRequestsAllowed
Microsoft Edge Network Settings > **Enable zstd content encoding support**	ZstdContentEncodingEnabled
Microsoft Edge Network Settings > **Specifies whether to block requests from public websites to devices on a user's local network** (deprecated)	LocalNetworkAccessRestrictionsEnabled

- **v139** - Intune supports the following new ADMX-backed policies for Microsoft Edge:

Expand table

Setting	CSP
Microsoft Edge > **Identity and sign-in** > **Prioritize app-specified profile to open external links**	EdgeOpenExternalLinksWithAppSpecifiedProfile
Microsoft Edge > **Extensions** > **Specify extensions users must allow in order to navigate using InPrivate mode**	MandatoryExtensionsForIncognitoNavigation
Microsoft Edge > **Control whether Microsoft 365 Copilot Chat shows in the Microsoft Edge for Business toolbar**	Microsoft365CopilotChatIconEnabled
Microsoft Edge > **Configuration policy for Microsoft Edge for Business Reporting Connectors**	OnSecurityEventEnterpriseConnector

Microsoft Edge > **Allow software WebGL fallback using SwiftShader**	EnableUnsafeSwiftShader

The following legacy settings are deprecated, and shouldn't be used:

⛶ **Expand table**

Setting	CSP
Microsoft Edge > **Controls whether the new HTML parser behavior for the `<select>` element is enabled**	SelectParserRelaxationEnabled
Microsoft Edge > **Enable keyboard focusable scrollers**	KeyboardFocusableScrollersEnabled

- Some existing policies have string updates that reflect the latest browser behavior and terminology.

OneDrive:

- **Disable a toast and activity center message to encourage a user to sign in OneDrive using an existing credential that is made available to Microsoft applications** - This setting allows IT admins to prevent detection of new accounts in OneDrive, helping enforce organizational sync and access controls.

Administrative Templates\Windows Components\Sync your settings:

- **Enable Windows Backup** - This setting allows IT admins to manage syncing behavior for Windows Backup features. Specifically, this policy controls whether language preferences are included in backup sync, which helps organizations tailor backup configurations to their needs.

Applies to:

✓ Windows

New day zero settings available in the Apple settings catalog

The Settings Catalog lists all the settings you can configure in a device policy, and all in one place. For more information about configuring Settings Catalog profiles in Intune, see Create a policy using settings catalog.

There are new settings in the Settings Catalog. To see these settings, in the Microsoft Intune admin center , go to **Devices** > **Manage devices** > **Configuration** > **Create** > **New policy** > **iOS/iPadOS** or **macOS** for platform > **Settings catalog** for profile type.

iOS/iPadOS

Declarative Device Management (DDM) > Audio Accessory Settings:

- Temporary Pairing Disabled
- Temporary Pairing Unpairing Time
- Unpairing Policy
- Unpairing Hour

Declarative Device Management (DDM) > Safari Settings:

- Accept Cookies
- Allow Disabling Fraud Warning
- Allow History Clearing
- Allow JavaScript
- Allow Private Browsing
- Allow Popups
- Allow Summary
- Page Type
- Homepage URL
- Extension Identifier

Restrictions:

- Allow Safari History Clearing
- Allow Safari Private Browsing
- Denied ICCIDs For iMessage And FaceTime
- Denied ICCIDs For RCS

macOS

Authentication > **Extensible Single Sign On Kerberos**:

- Allow Platform SSO Auth Fallback

Declarative Device Management (DDM) > **Safari Settings**:

- Allow History Clearing
- Allow Private Browsing
- Allow Summary
- Page Type
- Homepage URL
- Extension Identifier

Restrictions:

- Allow Safari History Clearing
- Allow Safari Private Browsing

New setting in the Android settings catalog

The Settings Catalog lists all the settings you can configure in a device policy, and all in one place. For more information about configuring Settings Catalog profiles in Intune, see Create a policy using settings catalog.

There's a new **Hide organization name** setting (**Devices** > **Manage devices** > **Configuration** > **Create** > **New policy** > **Android Enterprise** for platform > **Settings catalog** for profile type). When set to **True**, the enterprise name isn't shown on the device, such as lock screen.

For a list of existing settings you can configure in the settings catalog, see Android Enterprise device settings list in the Intune settings catalog.

Applies to:

✓ Android Enterprise corporate-owned devices with a work profile (COPE)
✓ Android Enterprise corporate owned fully managed (COBO)

Device enrollment

Intune supports Ubuntu 22.04 and later

Microsoft Intune and the Microsoft Intune app for Linux now support Ubuntu 22.04 LTS and Ubuntu 24.04 LTS. Support ended for Ubuntu 20.04 LTS. Devices that are currently enrolled on Ubuntu 20.04 LTS remain enrolled even though the version is no longer supported. New devices are unable to enroll if they're running Ubuntu 20.04 LTS. To see what devices or users might be affected, check your Intune reporting. In the admin center, go to **Devices **> **All devices** and filter OS by Linux. You can add more columns to help identify who in your organization has devices running Ubuntu 20.04 LTS. Notify your users to upgrade their devices to a supported Ubuntu version.

For more information about Linux enrollment, see Linux device enrollment guide for Microsoft Intune.

Device management

Wipe remote action supports Multi Admin Approval

When you use the Multi Admin Approval feature, you require a second admin account to approve a change before the change is applied.

The **Wipe** remote action supports Multi Admin Approval. Use Multi Admin Approval with the **Wipe** action to help mitigate the risk of unauthorized or compromised remote actions by a single admin account.

For more information on Multi Admin Approval, see Use Multi Admin Approval in Intune.

Configure Windows Backup for Organizations (public preview)

Intune administrators can configure a new feature in public preview called Windows Backup for Organizations. With this feature, you can back up your organization's Windows 10 or Windows 11 settings and restore them on a Microsoft Entra joined device. Backup settings are configurable in the Microsoft Intune admin center settings catalog, while a tenant-wide setting that lets you restore a device is available in the admin center under **Enrollment**. The backup setting is available now in public preview, while the restore setting will be available for public preview beginning August 26.

For more information about this feature, see Windows Backup for Organizations in Microsoft Intune.

New resolution button improves compliance remediation experience

We improved the Just in Time (JIT) compliance remediation experience for device users in Microsoft Intune. Intune collaborated with Microsoft Defender to:

- Remove user clicks required to view and learn remediation steps.
- Add a **Resolve** button to reduce time-to-remediation.

When a user opens a productivity app and sees they're marked noncompliant due to Microsoft Defender, the user can now select **Resolve.** This action redirects them to Microsoft Defender, where Microsoft Defender takes steps to remediate the user and then redirect the user back to their productivity app.

Even if you aren't using Microsoft Defender, if you have Conditional Access turned on your users can have an improved experience. With JIT compliance remediation, users go through an embedded flow that shows them their compliance status, noncompliance reasoning, and a list of actions right within a productivity app. This flow eliminates extra steps, the need to switch between apps, and reduces the number of authentications.

As an admin, if you have JIT registration and compliance remediation set up already, you have no action items. If you don't, set it up today to support this new functionality. For more information, see:

- Set up just-in-time registration.
- Update iOS device settings.

Intune apps

Newly available protected apps for Intune

The following protected apps are now available for Microsoft Intune:

- Avenza Maps for Intune by Avenza Systems Inc.
- Datasite for Intune by Datasite (Android)
- Dialpad by Dialpad, Inc.
- Dialpad Meetings by Dialpad, Inc.
- Omega 365 by Omega 365 Core AS
- Symphony Messaging Intune by Symphony Communication Services, LLC
- Zoho Projects - Intune by Zoho Corporation (Android)

For more information about protected apps, see Microsoft Intune protected apps.

Monitor and troubleshoot

Declarative software update reports for Apple devices

You can now use several new software update reports for Apple devices that are powered by Apples built-in declarative reporting infrastructure. The declarative reporting infrastructure provides Intune with a near real-time view of the software update status of managed devices. The following Apple software update reports are now available:

- A *per-device software update report* - Per-device software update reports are available in the Intune Admin center by going to *Devices* and then selecting an applicable device. In the Devices Overview pane for that device, below Monitor, you see the report listed as **iOS software updates** for iOS or iPadOS devices, and as **macOS software updates** for macOS devices.

  With these per-device reports available, the previously available macOS per-device **Software updates** report is now deprecated. While the deprecated report remains available in the admin center and can still be used while viewing a device, the report will be removed from Intune with a future update.

- **Apple software update failures** - With this operational report, you can view details across your entire managed Apple device fleet. Details include why the update failed to install and the timestamp of the last failure. To find this report, in the admin center go to *Devices* > *Monitor*, and then select the report's name to view the report details.

- **Apple software update report** - This report is an organizational report that displays details about pending and current software update information across your entire managed Apple device fleet. To find this report, in the admin center go to *Reports* > *Device management* > *Apple updates*, select the *Reports* tab, and then select the report tile.

- **Apple software update summary report** - View the Apple software update summary report, in the admin center go to *Reports* > *Device management* > *Apple updates*, and then select the *Summary* tab. You see a roll-up of update status from macOS, iOS, and iPadOS devices. This status includes the version of the latest update that's available for each platform, and the date that update became available.

The following Apple devices support these new reports:

- iOS 17 and later
- iPadOS 17 and later
- macOS 14 and later

For more information about the changes behind these reports, see Support tip: Move to declarative device management for Apple software updates .

Role-based access control

Multi Admin Approval support for role-based access control

Multi Admin Approval now supports role-based access control. When enabled, any changes to roles, including modifications to role permissions, admin groups, or member group assignments, require a second administrator to approve the change before it's applied. This dual authorization process helps protect your organization from unauthorized or accidental role-based access control changes.

For more information, see Role-based access control in Microsoft Intune.

Week of August 11, 2025

Device management

Platform SSO is generally available (GA) and also supports custom TGT

Platform SSO is a feature in Microsoft Entra that enables single sign-on (SSO) using a Microsoft Entra ID on macOS devices. Using the Intune settings catalog, you can configure Platform SSO and use Intune to deploy the Platform SSO configuration to your macOS devices.

- Microsoft Entra announced that Platform SSO for macOS devices is generally available (GA). For more information on this Microsoft Entra feature, see Microsoft Enterprise SSO plug-in for Apple devices.
- Microsoft Entra supports Kerberos Ticket Granting Tickets (TGTs) to access on-premises Active Directory and Microsoft Entra ID using Apple's Kerberos SSO extension .

  On the Company Portal version 5.2508.0 and newer, you can use the Intune settings catalog Platform SSO policy to enable Kerberos SSO to on-premises and cloud resources using the TGTs.

To configure Platform SSO in Intune, see:

- Configure Platform SSO for macOS devices in Intune
- Common Platform SSO scenarios for macOS devices in Intune

Applies to:

✓ macOS

Device security

Update required for Microsoft Tunnel endpoints

As part of our ongoing improvements to the Microsoft Tunnel infrastructure, we introduced new endpoints with the March 19, 2025 release. You must upgrade your Microsoft Tunnel to the March 19, 2025 release version or later to ensure you're using the new endpoints. Once you upgrade to this version or later, you can't downgrade to an earlier version. Earlier releases that rely on legacy endpoints aren't supported and might cause service disruptions. To continue with uninterrupted service, we recommend upgrading to the latest supported build and avoiding rollback to unsupported versions.

Week of July 28, 2025

Device management

New Microsoft Graph permissions for API calls to device management endpoints

Calls to several Microsoft Graph APIs now require one of two newer *DeviceManagement* permissions that replace the use of previously supported permissions. The following are the two new permissions and the original permissions that the new permissions replace:

- **DeviceManagementScripts.Read.All** - This new permission replaces use of *DeviceManagementConfiguration.Read.All*
- **DeviceManagementScripts.ReadWrite.All** - This new permission replaces use of the *DeviceManagementConfiguration.ReadWrite.All*

Access to the following Microsoft Graph API calls now require using the new permissions:

- ~/deviceManagement/deviceShellScripts
- ~/deviceManagement/deviceHealthScripts
- ~/deviceManagement/deviceComplianceScripts
- ~/deviceManagement/deviceCustomAttributeShellScripts
- ~/deviceManagement/deviceManagementScripts

Currently both the *DeviceManagementScripts* and the older *DeviceManagementConfiguration* permissions remain functional. However, in early September 2025, tools and scripts that rely on the older permissions to access the listed APIs fail to function.

For more information, see How to use Microsoft Entra ID to access the Intune APIs in Microsoft Graph.

Week of July 21, 2025 (Service release 2507)

Microsoft Intune Suite

Endpoint Privilege Management support for wildcards in elevation rules

You can now use wildcards in the file name and file path of elevation rules you define for Endpoint Privilege Management (EPM). Wildcards allow for more flexible rule creation with broader matching capabilities, enabling file elevations for trusted files that have names that might change with subsequent revisions.

For file names, use of wildcards is supported only in the file name and not for the file extension. You can use a question mark `?` to replace a single character at any point in the file name and an asterisk `*` to replace a string of characters at the end of the file name.

The following are a few examples of wildcard use for a Visual Studio setup file called `VSCodeUserSetup-arm64-1.99.2.exe` found in `C:\Users\<username>\Downloads\`:

- File name:
  - `VSCodeUserSetup*.exe`
  - `VSCodeUserSetup-arm64-*.exe`
  - `VSCodeUserSetup-?????-1.??.?.exe`
- File path:
  - `C:\Users\*\Downloads\`

For more information, see Use variables in elevation rules in Configure policies for Endpoint Privilege Management.

App management

Newly available OEMConfig apps in Intune

The following OEMConfig app is now available in Intune for Android Enterprise:

- RugGear

For more information about OEMConfig, see Use and manage Android Enterprise devices with OEMConfig in Microsoft Intune.

Device configuration

New settings available in the Apple settings catalog

The Settings Catalog lists all the settings you can configure in a device policy, and all in one place. For more information about configuring Settings Catalog profiles in Intune, see Create a policy using settings catalog.

There are new settings in the Settings Catalog. To see these settings, in the Microsoft Intune admin center , go to **Devices** > **Manage devices** > **Configuration** > **Create** > **New policy** > **iOS/iPadOS** or **macOS** for platform > **Settings catalog** for profile type.

iOS/iPadOS

Cellular Private Network:

- Cellular Data Preferred
- CSG Network Identifier
- Data Set Name
- Enable NR Standalone
- Geofences
- Network Identifier
- Version Number

macOS

Microsoft Edge:

- The Microsoft Edge category is updated with new settings. Learn more about available macOS settings for Microsoft Edge at Microsoft Edge - Policies.

Device management

Platform support for Device Cleanup rules

Using cleanup rules, you can configure Intune to automatically clean up devices that appear to be inactive, stale, or unresponsive.

With this feature, you can:

- Configure individual device cleanup rules per platform, like Windows, iOS/iPadOS, macOS, and Android.
- Use the Audit logs to see the devices that the device cleanup rules conceal from the Intune reports.
- Use role-based access control (RBAC) to customize the user roles that can create device cleanup rules.

For more information, see device cleanup rules.

Device security

macOS support for local administrator account configuration with password solution - GA

macOS automated device enrollment (ADE) profiles can configure newly enrolled macOS devices that run macOS 12 or later with both a local administrator and local user account, along with support for the Microsoft Local Admin Password Solution (LAPS).

With this support:

- You can use macOS automated device enrollment (ADE) profiles to configure the local administrator and user accounts for a device. When configured, this capability applies to all new macOS device enrollments and device re-enrollments assigned to that enrollment profile.

- Intune creates a randomized, unique, and secure password for the device's admin account. It's 15 alphanumeric characters.
- Intune automatically rotates the password every six months by default.
- Previously enrolled devices aren't affected unless they re-enroll with Intune through an applicable ADE profile.

For account creation, the profile supports the following variables:

- **Admin account username**:
  - {{serialNumber}} - for example, F4KN99ZUG5V2
  - {{partialupn}} - for example, John.Dupont
  - {{managedDeviceName}} - for example, F2AL10ZUG4W2_14_4/15/2025_12:45PM
  - {{onPremisesSamAccountName}} - for example, JDoe

- **Admin account full name**:
  - {{username}} - for example, John@contoso.com
  - {{serialNumber}} - for example, F4KN99ZUG5V2
  - {{onPremisesSamAccountName}} - for example, JDoe

To support LAPS:

- There are two new role-based access control permissions for *Enrollment program* that can grant an administrative account permission to view a managed devices password, and to rotate that password.
- By default, these permissions aren't part of any built-in Intune RBAC role, and must be explicitly assigned to admins through custom roles.

To learn about all the details for this new capability, see Configure support for macOS ADE local account configuration with LAPS in Microsoft Intune.

Intune apps

Newly available protected apps for Intune

The following protected apps are now available for Microsoft Intune:

- Vault CRM by Veeva Systems Inc. (iOS)

- Workvivo by Workvivo

For more information about protected apps, see Microsoft Intune protected apps.

Week of July 14, 2025

Device management

Experience Microsoft Copilot in Intune

You can now use Microsoft Copilot in Intune to explore your Intune data using natural language, take action on the results, manage policies and settings, understand your security posture, troubleshoot device issues, and view insights about enrolled Surface devices.

- **Explore your Intune data** - Use natural language to explore your Intune data and take action based on the results. Admins can run queries against Intune resource data, including questions about devices, apps, policies, updates, and compliance. When a query runs, a Copilot summary helps you understand the results and offers suggestions. You can add devices or users from the query results to a group to target apps and policies. There are also example queries that you can filter to find an example that best matches your request or use to help you create your own request.

  Data coverage, querying capabilities, and actionability will evolve over time as we make improvements to how you explore your data.

  To learn more about this feature, see Explore Intune data with natural language and take action.

- **Conversational chat experience** - Use the Copilot in Intune chat experience to interact with your data using natural language to manage tasks, get insights, and troubleshoot issues. Here's what you can do with the chat experience:
  - Policy and setting management: Use Copilot in Intune to summarize an existing policy or learn more about individual policy settings and recommended values.
  - Device details and troubleshooting: Use Copilot in Intune to get device details and troubleshoot a device to get device-specific information like the installed apps, group memberships and more.

  - Device Query: Use Copilot in Intune to help you create Kusto Query Language (KQL) queries to run when using device query in Intune.
  - Endpoint Privilege Management (EPM): Use Copilot in Intune to help identify potential elevation risks from within the EPM support approved workflow.

- **Microsoft Copilot in Surface Management Portal** - Microsoft Copilot in Intune includes the Surface Management Portal, a workspace in the Intune admin center that brings together vital data and insights about enrolled Surface devices, all in one place.
  - Gain insights into device compliance, support activity, applicable warranty or protection plan coverage, and carbon emission estimates.
  - Monitor the status of each device, including applicable warranty or protection plan expirations and active support requests.
  - Centralize Surface-specific device administration in a single environment.
  - Automatically access comprehensive information from your Intune-enrolled Surface devices, which flows into the Surface Management Portal when users sign in for the first time.

  To learn more about this feature, see Security Copilot in Microsoft Surface Management Portal.

Monitor and troubleshoot

Export device query results to CSV file

Now after running a multiple-device query, you can export up to 50,000 query results to a CSV file. For more information, see How to use device query for multiple devices.

Week of June 23, 2025 (Service release 2506)

App management

Microsoft Intune support for Apple AI features

Intune app protection policies have new standalone settings for Apple AI features (Genmojis, Writing tools, and screen capture). Apps running the following Intune App SDK and App Wrapping Tool versions support the standalone settings:

- Xcode 15 version 19.7.12 or later
- Xcode 16 version 20.4.0 or later

Previously, these Apple AI features were blocked when the app protection policy **Send Org data to other apps** setting is configured to a value other than **All apps**.

For more information about Intune's related app protection policies, see iOS app protection policy settings.

Add Enterprise App Catalog apps to ESP blocking apps list

Windows Autopilot now supports Enterprise App Catalog apps. Microsoft Intune Enterprise App Management enables IT admins to easily manage applications from the Enterprise App Catalog. Using Windows Autopilot, you can select apps from the Enterprise App Catalog as blocking apps in the Enrollment Status Page (ESP) and the Device Preparation Page (DPP) profiles. This feature allows you to ensure those apps are delivered before the user can access the desktop.

For related information, see Set up the Enrollment Status Page, Overview of Windows Autopilot device preparation, and Add an Enterprise App Catalog app to Microsoft Intune.

Applies to:

✓ Windows

Managed Home Screen orientation changes with Android 16

Starting with Android 16, Android stops enforcing screen orientation on devices with 600 dp and larger display settings. This change impacts the Managed Home Screen (MHS) on devices with larger form factors, like tablets.

On these Android 16 devices, orientation is determined by the device's orientation setting, not the MHS settings you configure.

To learn more about Android 16 changes, see Behavior changes: Apps targeting Android 16 or higher (opens Android website).

Applies to:

✓ Android Enterprise

Device configuration

New settings available in the Apple settings catalog

The Settings Catalog lists all the settings you can configure in a device policy, and all in one place. For more information about configuring settings catalog profiles in Intune, see Create a policy using settings catalog.

There are new settings in the settings catalog. To see these settings, in the Microsoft Intune admin center, go to **Devices** > **Manage devices** > **Configuration** > **Create** > **New policy** > **iOS/iPadOS** or **macOS** for platform > **Settings catalog** for profile type.

iOS/iPadOS

Managed Settings:

- Idle Reboot Allowed

macOS

Authentication > **Extensible Single Sign On (SSO)**:

- Allow Device Identifiers In Attestation

Microsoft Edge:

- The Microsoft Edge category has hundreds of new settings. Learn more about available macOS Edge settings at Microsoft Edge - Policies.

Apple deprecated the Identification payload in macOS 15.4.

New Block Bluetooth setting in the Android Enterprise settings catalog

The Settings Catalog lists all the settings you can configure in a device policy, and all in one place. For more information about configuring Settings Catalog profiles in Intune, see Create a policy using settings catalog.

There's a new **Block Bluetooth** setting (**Devices** > **Manage devices** > **Configuration** > **Create** > **New policy** > **Android Enterprise** for platform > **Settings catalog** for profile type). When set to **True**, Bluetooth is disabled on the device.

There's also a **Block Bluetooth Configuration** setting that prevents end users from changing the Bluetooth setting on the device.

These settings are different and have different results. Some examples include:

- **Scenario**: An end user turned on the Bluetooth setting on their device. The admin creates an Intune policy that sets the **Block Bluetooth** setting to **True**.

  In this situation, Bluetooth is blocked on the device, even though the end user turned it on.

- **Scenario**: An end user turned on the Bluetooth setting on their device. The admin creates an Intune policy that sets the **Block Bluetooth Configuration** setting to **True**.

  In this situation, Bluetooth is turned on since the end user previously turned it on. The end user can't turn off Bluetooth. If the end user previously turned Bluetooth off, and then the **Block Bluetooth Configuration** policy applies, then Bluetooth is turned off and the end user can't turn it back on.

For a list of existing settings you can configure in the settings catalog, see Android Enterprise device settings list in the Intune settings catalog.

Applies to:

✓ Android Enterprise corporate-owned devices with a work profile (COPE)
✓ Android Enterprise corporate owned fully managed (COBO)
✓ Android Enterprise corporate owned dedicated devices (COSU)

Device management

New reporting system for improved performance and data consistency

Microsoft Intune is rolling out the new Policy Reporting Service (PRS) V3. The new system brings faster report generation, improved reliability, and better data consistency.

In the first phase, some high-traffic compliance and device configuration reports are transitioning to the new system.

Users notice quicker updates in the Intune admin center and fewer issues with stale data. No action is required from users, as your reports transition automatically.

With (PRS) V3, device reports only update when a device checks in. This behavior is an intentional change from previous versions.

If a policy is removed but the device hasn't checked in, the report continues to show the last known status. The policy is removed during the next check-in, at which point the report is updated. This behavior improves accuracy but can differ from what customers experienced with (PRS) V1.

To learn more about the Intune reports you can use, see Intune reports.

Device security

New attributes and S/MIME baseline requirements for SCEP certificate profiles

Intune supports two new attributes for subject name settings in SCEP and PKCS device configuration profiles. They include:

- G={{GivenName}}
- SN={{SurName}}

Beginning July 16, if you're using a third party public certificate authority (CA) integrated with the Intune SCEP API for issuing S\MIME (encryption or signing) certificates anchored up to a public root CA, then you must use these attributes in the subject name format. After that date, a public CA won't issue or sign S\MIME certificates that omit these attributes.

For more information, see S/MIME certificate requirements for third party public CA.

Intune apps

Newly available protected apps for Intune

The following protected apps are now available for Microsoft Intune:

- Datasite for Intune by Datasite (iOS)
- Mijn InPlanning by Intus Workforce Solutions (iOS)
- Nitro PDF Pro by Nitro Software, Inc. (iOS)
- SMART TeamWorks by SMART Technologies ULC (iOS)

For more information about protected apps, see Microsoft Intune protected apps.

Monitor and troubleshoot

New status column in Windows hardware attestation report

We added a new column, **Attest Status**, to the Windows hardware attestation report to improve visibility into attestation errors. This column shows error messages received during the attestation process, helping you identify issues from both the service and client sides. Error types shown in this column include:

- WinINet errors
- HTTP bad request errors
- Other attestation-related failures

For more information about the report, see Windows hardware attestation report.

Week of June 9, 2025

App management

ARM64 support for Win32 apps

When adding a Win32 app to Intune, you can select an option to check and install the app on Windows devices running ARM64 operating systems. This capability is available from the Microsoft Intune admin center by selecting **Apps** > **All apps** > **Create**. The ARM64 option is available by selecting the **Operating system architecture** option under the **Requirements** step. To ensure that you don't have any impact to any Win32 applications that you previously targeted to 64-bit devices, your existing 64-bit Win32 applications also have ARM64 selected. After the availability of being able to specifically target ARM64 operating system architectures, selecting x64 won't target ARM64 devices.

For related information, see Win32 app management in Microsoft Intune.

Applies to:

- ✓ Windows devices

Week of June 2, 2025

Device security

Vulnerability Remediation Agent for Intune (public preview)

The Vulnerability Remediation Agent is currently in a limited public preview and available to only a select group of customers. If you're interested in gaining access or would like to learn more, please reach out to your sales team for further details and next steps.

When run, this agent uses data from Microsoft Defender Vulnerability Management to identify and then provide remediation guidance for vulnerabilities on your managed devices. You run and access the agent and view its results from within the Intune admin center where you see suggestions prioritized by the agent for remediation. Each suggestion includes key information like associated CVEs, severity, exploitability, affected systems, organizational exposure, business impact, and remediation guidance.

This information empowers you with a current assessment of potential risk to your environment and guidance to help you decide which risk to address first.

For more information about this agent including prerequisites, see Vulnerability Remediation Agent for Security Copilot in Microsoft Intune.

Week of May 26, 2025 (Service release 2505)

Microsoft Intune Suite

Endpoint Privilege Management rules explicitly deny elevation

Endpoint Privilege Management (EPM) elevation rules now include a new file elevation type of **Deny**. An EPM elevation rule set to *Deny* blocks the specified file from running in an elevated context. We recommend using file elevation rules to allow users to elevate specific files. But, a deny rule can help you ensure that certain files like known and potentially malicious software can't be run in an elevated context.

Deny rules support the same configuration options as other elevation types except for child processes, which aren't used.

For more information about EPM, which is available as an Intune Suite add-on-capability, see Endpoint Privilege Management overview.

App management

Newly available protected apps for Intune

The following protected apps are now available for Microsoft Intune:

- Windows App by Microsoft Corporation (Android)
- Microsoft Clipchamp by Microsoft Corporation (iOS)

- 4CEE Connect by 4CEE Development
- Mobile Helix Link for Intune by Mobile Helix

For more information about protected apps, see Microsoft Intune protected apps.

Device configuration

Manage DFCI profiles for Windows devices

You can use DFCI profiles to manage UEFI (BIOS) settings for NEC devices that run Windows 10 or Windows 11. Not all NEC devices running Windows are enabled for DFCI. Contact your device vendor or device manufacturer for eligible devices.

You can manage DFCI profiles from within the Microsoft Intune admin center by going to **Devices** > **Manage devices** > **Configuration** > **Create** > **New policy** > **Windows 10 and later** for platform > **Templates** > **Device Firmware Configuration Interface** for profile type. For more information about DFCI profiles, see:

- Configure Device Firmware Configuration Interface (DFCI) profiles on Windows devices in Microsoft Intune
- Device Firmware Configuration Interface (DFCI) management with Windows Autopilot

Applies to:

✓ Windows

Device enrollment

Custom naming template for AOSP devices

Use a custom template for naming AOSP user-affiliated and userless devices when they enroll with Intune. The template is available to configure in the enrollment profile. It can contain a combination of free text and predefined variables (like device serial number, device type), and for user-affiliated devices, the owner's username. For more information about how to configure the template, see:

- Set up Intune enrollment for Android (AOSP) corporate-owned userless devices
- Set up Intune enrollment for Android (AOSP) corporate-owned user-associated devices

Change to role-based access control for device enrollment limits

We updated role-based access control (RBAC) for device limits. If you're currently assigned the policy and profile manager role, or the *device configurations* permissions that are built-in to the role, you now have read-only access to device enrollment limit policies. To create and edit these policies, you must be an Intune Administrator.

Device management

Cross Platform Device Inventory

Android, iOS, and Mac devices are added to device inventory. Intune now collects a default set of inventory data including 74 Apple properties and 32 Android properties.

For more information, see View device details with Microsoft Intune.

Enhanced security during unattended Remote Help sessions on Android devices

During an unattended Remote Help sessions on Android devices, the screen of the device is blocked and users are notified if they interact with it. This feature enhances the security and user awareness during remote assistance.

This feature is for Zebra and Samsung devices that enrolled as Android Enterprise corporate owned dedicated devices.

For more information on Remote Help, see Remote Help.

Device security

Detect rooted corporate-owned Android Enterprise devices

Configure compliance policies to detect if a corporate-owned Android Enterprise device is rooted. If Microsoft Intune detects that a device is rooted, you can mark it as noncompliant. This feature is now available for devices enrolled as fully managed, dedicated, or corporate-owned with a work profile. For more information, see Device compliance settings for Android Enterprise in Intune.

To learn about root detection support for Microsoft Defender on Android, see Key capabilities in Microsoft Defender for Endpoint in the Defender documentation, and the Defender for Endpoint blog Native root detection support for Microsoft Defender on Android .

Applies to:

✓ Android

New endpoint security profile for configuring Endpoint detection and response and Antivirus exclusion settings on Linux devices

As part of the Intune scenario for Microsoft Defender for Endpoint security settings management, you can use a new *Endpoint detection and response* profile for Linux named **Microsoft Defender Global Exclusions (AV+EDR)** that you can now use to manage Linux device exclusions for both Microsoft Defender *Endpoint detection and response* (EDR) and *Antivirus* (AV).

This profile supports settings related to global exclusion settings as detailed in Configure and validate exclusions on Linux in the Microsoft Defender documentation. These exclusion configurations can apply to both the antivirus and EDR engines on the Linux client to stop associated real time protection EDR alerts for excluded items. Exclusions can be defined by the file path, folder, or process explicitly defined by the admin in the policy.

The new Intune profile:

- Is available in addition to the existing endpoint security Antivirus policy for Microsoft Defender Antivirus.
- Is supported for devices you manage through the Microsoft Defender for Endpoint

security settings management scenario.
- Isn't supported for Linux devices managed directly by Intune.

For details about the available Defender settings, see Configure security settings in Microsoft Defender for Endpoint on Linux - Microsoft Defender for Endpoint in the Defender for Endpoint documentation.

Applies to:

✓ Linux

Tenant administration

Data collection from SimInfo entity on Windows devices

You can now collect data from the SimInfo entity on Windows devices with enhanced device inventory. For more information, see Intune Data Platform.

Applies to:

✓ Windows

Week of April 28, 2025

App management

Intune support for Apple specialty devices

App protection policies (APP) support Microsoft Edge (v136 or later), OneDrive (v16.8.4 or later), and Outlook (v4.2513.0 or later). To enable this setting for these specific apps on visionOS devices, you must set `com.microsoft.intune.mam.visionOSAllowiPadCompatApps to Enabled` in your app configuration policy. Once you assign your app configuration policy, you can create and assign your app protection policy for your VisionOS devices. For more information, see Protect data on VisionOS devices.

Tenant administration

New icon for Microsoft Intune

Microsoft Intune has a new icon. The Intune icon is being updated across platforms and apps associated with Intune, such as the Intune admin center and Intune Company Portal app. The new icon will gradually be implemented over the next few months.

What's new archive

For previous months, see the What's new archive.

Notices

These notices provide important information that can help you prepare for future Intune changes and features.

Update to the latest Intune Company Portal for Android, Intune App SDK for iOS, and Intune App Wrapper for iOS

Starting **January 19, 2026**, or soon after, we're making updates to improve the Intune mobile application management (MAM) service. To stay secure and run smoothly, this update will require iOS wrapped apps, iOS SDK integrated apps, and the Intune Company Portal for Android to be updated to the latest versions.

> ⓘ **Important**
>
> If you don't update to the latest versions, users will be blocked from launching your app.

The way Android updates, once one Microsoft application with the updated SDK is on the device and the Company Portal is updated to the latest version, Android apps will update, so this message is focused on iOS SDK/app wrapper updates. We recommend to always update your Android and iOS apps to the latest SDK or app wrapper to ensure that your app continues to run smoothly. Review the following GitHub announcements for more details on the specific effect:

- SDK for iOS: Action Required: Update the MAM SDK in your application to avoid end user impact - microsoftconnect/ms-intune-app-sdk-ios Discussion #598 | GitHub
- Wrapper for iOS: Action Required: Wrap your application with version 20.8.1+ to avoid end user impact - microsoftconnect/intune-app-wrapping-tool-ios Discussion #143 | GitHub

If you have questions, leave a comment on the applicable GitHub announcement.

How does this change affect you or your users?

If your users haven't updated to the latest Microsoft or third-party app protection supported apps, they'll be blocked from launching their apps. If you have iOS line-of-business (LOB) applications that are using the Intune wrapper or Intune SDK, you must be on Wrapper/SDK version **20.8.0** or later for apps compiled with Xcode 16 and version **21.1.0** or later for apps compiled with Xcode 26 to avoid your users being blocked.

How can you prepare?

Plan to make the following changes before **January 19, 2026**:

- For apps using the Intune App SDK, you must update to the new version of the Intune App SDK for iOS:
  - For apps built with XCode 16 use v20.8.0 - Release 20.8.0 - microsoftconnect/ms-intune-app-sdk-ios | GitHub
  - For apps built with XCode 26 use v21.1.0 - Release 21.1.0 - microsoftconnect/ms-intune-app-sdk-ios | GitHub

- For apps using the wrapper, you must update to the new version of the Intune App Wrapping Tool for iOS:
  - For apps built with XCode 16 use v20.8.1 - Release 20.8.1 - microsoftconnect/intune-app-wrapping-tool-ios | GitHub
  - For apps built with XCode 26 use v21.1.0 - Release 21.1.0 - microsoftconnect/intune-

app-wrapping-tool-ios | GitHub

- For tenants with policies targeted to iOS apps:
  - Notify your users that they need to upgrade to the latest version of the Microsoft apps. You can find the latest version of the apps in the App store . For example, you can find the latest version of Microsoft Teams here and Microsoft Outlook here .
  - Additionally, you can enable the following Conditional Launch settings:
    - The **Min SDK version** setting to block users if the app is using Intune SDK for iOS older than 20.8.0.
    - The **Min app version** setting to warn users on older Microsoft apps. Note, this setting must be in a policy targeted to only the targeted app.
- For tenants with policies targeted to Android apps:
  - Notify your users that they need to upgrade to the latest version (v5.0.6726.0) of the Intune Company Portal app.
  - Additionally, you can enable the following Conditional Launch device condition setting:
    - The **Min Company Portal version** setting to warn users using a Company Portal app version older than 5.0.6726.0.

> ⓘ **Note**
>
> Use Conditional Access policy to ensure that only apps with app protection policies can access corporate resources. For more information, see the Require approved client apps or app protection policy with mobile devices on creating Conditional Access policies.

Update firewall configurations to include new Intune network endpoints

As part of Microsoft's ongoing Secure Future Initiative (SFI) , starting on or shortly after **December 2, 2025**, the network service endpoints for Microsoft Intune will also use the Azure Front Door IP addresses. This improvement supports better alignment with modern security practices and over time will make it easier for organizations using multiple Microsoft products to manage and maintain their firewall configurations. As a result, customers might be required to add these network (firewall) configurations in third-party applications to enable proper function of Intune device and app management. This change will affect customers using a firewall allowlist that allows outbound traffic based on IP addresses or Azure service tags.

Don't remove any existing network endpoints required for Microsoft Intune. More network endpoints are documented as part of the Azure Front Door and service tags information referenced in the following files:

- Public clouds: Download Azure IP Ranges and Service Tags – Public Cloud from Official Microsoft Download Center
- Government clouds: Download Azure IP Ranges and Service Tags – US Government Cloud from Official Microsoft Download Center

The other ranges are in the JSON files linked above and can be found by searching for "AzureFrontDoor.MicrosoftSecurity".

How does this change affect you or your users?

If you've configured an outbound traffic policy for Intune IP address ranges or Azure service tags for your firewalls, routers, proxy servers, client-based firewalls, VPN, or network security groups, you'll need to update them to include the new Azure Front Door ranges with the "AzureFrontDoor.MicrosoftSecurity" tag.

Intune requires internet access for devices under Intune management, whether for mobile device management or mobile application management. If your outbound traffic policy doesn't include the new Azure Front Door IP address ranges, users can face sign-in issues, devices might lose connectivity with Intune, and access to apps like the Intune Company Portal or the apps protected by app protection policies could be disrupted.

How can you prepare?

Ensure that your firewall rules are updated and added to your firewall's allowlist with the other IP addresses documented under Azure Front Door by **December 2, 2025**.

Alternatively, you can add the `AzureFrontDoor.MicrosoftSecurity` service tag to your firewall rules to allow outbound traffic on port 443 for the addresses in the tag.

If you aren't the IT admin who can make this change, notify your networking team. If you're responsible for configuring internet traffic, see the following documentation for more details:

- Azure Front Door
- Azure service tags
- Intune network endpoints
- US government network endpoints for Intune

If you have a helpdesk, inform them about this upcoming change.

Update to support statement for Windows 10 in Intune

Windows 10 has reached end of support on **October 14, 2025**. Windows 10 no longer receives quality or feature updates. Security updates are only available to commercial customers who have enrolled devices into the Extended Security Updates (ESU) program. For more details, review the following additional information.

How does this change affect you or your users?

Microsoft Intune continues to maintain core management functionality for Windows 10, including:

- Continuity of device management.
- Support for updates and migration workflows to Windows 11.
- Ability for ESU customers to deploy Windows security updates and maintain secure patch levels.

The final release of Windows 10 (version 22H2) is designated as an "allowed" version in Intune. While updates and new features are not available, devices running this version can still enroll in Intune and use eligible features, but functionality is not guaranteed and can vary.

How can you prepare?

Use the **All devices** report in the Intune admin center to identify devices still running Windows 10 and upgrade eligible devices to Windows 11.

If devices cannot be upgraded in time, consider enrolling eligible devices in the Windows 10 ESU program to continue receiving critical security updates.

Additional information

- Stay secure with Windows 11, Copilot+ PCs, and Windows 365 before support ends for Windows 10
- Windows 10 reaching end of support
- Enable Extended Security Updates (ESU)
- Windows 10 release information
- Windows 11 release information
- Lifecycle FAQ - Windows

Plan for Change: Intune is moving to support iOS/iPadOS 17 and later

Later in calendar year 2025, we expect iOS 26 and iPadOS 26 to be released by Apple. Microsoft Intune, including the Intune Company Portal and Intune app protection policies (APP, also known as MAM), requires iOS 17/iPadOS 17 and higher shortly after the iOS/iPadOS 26 release.

How does this change affect you or your users?

If you're managing iOS/iPadOS devices, you might have devices that won't be able to upgrade to the minimum supported version (iOS 17/iPadOS 17).

Given that Microsoft 365 mobile apps are supported on iOS 17/iPadOS 17 and higher, this change might not affect you. You likely already upgraded your OS or devices.

To check which devices support iOS 17 or iPadOS 17 (if applicable), see the following Apple documentation:

- Supported iPhone models
- Supported iPad models

> ⓘ **Note**
>
> Userless iOS and iPadOS devices enrolled through Automated Device Enrollment (ADE) have a slightly nuanced support statement due to their shared usage. The minimum supported OS version changes to iOS 17/iPadOS 17 while the allowed OS version changes to iOS 14/iPadOS 14 and later. For more information, see this statement about ADE Userless support .

How can you prepare?

Check your Intune reporting to see what devices or users might be affected. For devices with mobile device management (MDM), go to **Devices** > **All devices** and filter by OS. For devices with app protection policies, go to **Apps** > **Monitor** > **App protection status** and use the *Platform* and *Platform version* columns to filter.

To manage the supported OS version in your organization, you can use Microsoft Intune controls for both MDM and APP. For more information, see Manage operating system versions with Intune.

Plan for change: Intune is moving to support macOS 14 and higher later this year

Later in calendar year 2025, we expect macOS Tahoe 26 to be released by Apple. Microsoft Intune, the Company Portal app, and the Intune mobile device management agent support macOS 14 and later. Since the Company Portal app for iOS and macOS are a unified app, this change will occur shortly after the release of macOS 26. This change doesn't affect existing enrolled devices.

How does this change affect you or your users?

This change only affects you if you currently manage, or plan to manage, macOS devices with Intune. If your users have likely already upgraded their macOS devices, then this change might not affect you. For a list of supported devices, refer to macOS Sonoma is compatible with these computers.

> ⓘ **Note**
>
> Devices that are currently enrolled on macOS 13.x or below will continue to remain enrolled even when those versions are no longer supported. New devices are unable to enroll if they're running macOS 13.x or below.

How can you prepare?

Check your Intune reporting to see what devices or users might be affected. Go to **Devices** > **All devices** and filter by macOS. You can add more columns to help identify who in your organization has devices running macOS 13.x or earlier. Ask your users to upgrade their devices to a supported OS version.

Plan for Change: Google Play strong integrity definition update for Android 13 or above

Google recently updated the definition of "Strong Integrity" for devices running Android 13 or above, requiring hardware-backed security signals and recent security updates. For more information, see the Android Developers Blog: Making the Play Integrity API faster, more resilient, and more private. Microsoft Intune will enforce this change by **September 30, 2025**. Until then, we've adjusted app protection policy and compliance policy behavior to align with Google's recommended backward compatibility guidance to minimize disruption as detailed in Improved verdicts in Android 13 and later devices | Google Play | Android Developers.

How does this change affect you or your users?

If you have targeted users with app protection policies and/or compliance policies that are using devices running Android 13 or above without a security update in the past 12 months, these devices will no longer meet the "Strong Integrity" standard.

User impact - For users running devices on Android 13 or above after this change:

- Devices without the latest security updates might be downgraded from "Strong Integrity" to "Device Integrity", which could result in conditional launch blocks for affected devices.
- Devices without the latest security updates might see their devices become noncompliant in the Intune Company Portal app and could lose access to company resources based on your organization's Conditional Access policies.

Devices running Android versions 12 or below aren't affected by this change.

How can you prepare?

Before September 30, 2025, review and update your policies as needed. Ensure users with devices running Android 13 or above are receiving timely security updates. You can use the app protection status report to monitor the date of the last Android Security Patch received by the device and notify users to update as needed. The following admin options are available to help warn or block users:

- For app protection policies, configure the **Min OS version** and **Min patch version** conditional launch settings. For more details, review Android app protection policy settings in Microsoft Intune | Microsoft Learn
- For compliance policies, configure the **Minimum security patch level** compliance setting. For more details, review: Device compliance settings for Android Enterprise in Intune

Plan for Change: New Intune connector for deploying Microsoft Entra hybrid joined devices using Windows Autopilot

As part of Microsoft's Secure Future Initiative, we recently released an update to the Intune Connector for Active Directory to use a Managed Service Account instead of a local SYSTEM account for deploying Microsoft Entra hybrid joined devices with Windows Autopilot. The new connector aims to enhance security by reducing unnecessary privileges and permissions associated with the local SYSTEM account.

ⓘ **Important**

At the end of June 2025, we'll remove the old connector that uses the local SYSTEM account. At that point, we will stop accepting enrollments from the old connector. For more information, see the Microsoft Intune Connector for Active Directory security update blog.

How does this change affect you or your users?

If you have Microsoft Entra hybrid joined devices using Windows Autopilot, you need to transition to the new connector to continue deploying and managing devices effectively. If you don't update to the new connector, you won't be able to enroll new devices using the old connector.

How can you prepare?

Update your environment to the new connector by following these steps:

1. Download and install the new connector in the Intune admin center.
2. Sign in to set up the Managed Service Account (MSA).
3. Update the ODJConnectorEnrollmentWizard.exe.config file to include the required Organizational Units (OUs) for domain join.

For more detailed instructions, review: Microsoft Intune Connector for Active Directory security update and Deploy Microsoft Entra hybrid joined devices by using Intune and Windows Autopilot.

Plan for Change: New settings for Apple AI features; Genmojis, Writing tools, Screen capture

Today, the Apple AI features for Genmojis, Writing tools, and screen capture are blocked when the app protection policy (APP) "Send Org data to other apps" setting is configured to a value other than "All apps". For more details on the current configuration, app requirements, and the list of current Apple AI controls review the blog: Microsoft Intune support for Apple Intelligence

In an upcoming release, Intune app protection policies have new standalone settings for blocking screen capture, Genmojis, and Writing tools. These standalone settings are supported by apps that have updated to version 19.7.12 or later for Xcode 15 and 20.4.0 or later for Xcode 16 of the Intune App SDK and App Wrapping Tool.

How does this change affect you or your users?

If you configured the APP "Send Org data to other apps" setting to a value other than "All apps", then the new "Genmoji", "Writing Tools" and "Screen capture" settings are set to **Block** in your app protection policy to prevent changes to your current user experience.

> ⓘ **Note**
>
> If you configured an app configuration policy (ACP) to allow for screen capture, it overrides the APP setting. We recommend updating the new APP setting to **Allow** and removing the ACP setting. For more information about the screen capture control, review iOS/iPadOS app protection policy settings | Microsoft Learn.

How can you prepare?

Review and update your app protection policies if you'd like more granular controls for blocking or allowing specific AI features. (**Apps** > **Protection** > *select a policy* > **Properties** > **Basics** > **Apps** > **Data protection**)

Plan for change: User alerts on iOS for when screen capture actions are blocked

In an upcoming version (20.3.0) of the Intune App SDK and Intune App Wrapping Tool for iOS, support is added to alert users when a screen capture action (including recording and mirroring) is detected in a managed app. The alert is only visible to users if you have configured an app protection policy (APP) to block screen capture.

How does this change affect you or your users?

If APP has been configured to block screen capturing, users see an alert indicating that screen capture actions are blocked by their organization when they attempt to screenshot, screen record, or screen mirror.

For apps that have updated to the latest Intune App SDK or Intune App Wrapping Tool versions, screen capture is blocked if you configured "Send Org data to other apps" to a value other than "All apps". To allow screen capture for your iOS/iPadOS devices, configure the Managed apps app configuration policy setting "com.microsoft.intune.mam.screencapturecontrol" to **Disabled**.

How can you prepare?

Update your IT admin documentation and notify your helpdesk or users as needed. You can learn more about blocking screen capture in the blog: New block screen capture for iOS/iPadOS MAM protected apps

Plan for Change: Blocking screen capture in the latest Intune App SDK for iOS and Intune App Wrapping Tool for iOS

We recently released updated versions of the Intune App SDK and the Intune App Wrapping Tool. Included in these releases (v19.7.5+ for Xcode 15 and v20.2.0+ for Xcode 16) is the support for blocking screen capture, Genmojis, and writing tools in response to the new AI features in iOS/iPadOS 18.2.

How does this change affect you or your users?

For apps that have updated to the latest Intune App SDK or Intune App Wrapping Tool versions screen capture will be blocked if you configured "Send Org data to other apps" to a value other than "All apps". To allow screen capture for your iOS/iPadOS devices, configure the Managed apps app configuration policy setting "com.microsoft.intune.mam.screencapturecontrol" to **Disabled**.

How can you prepare?

Review your app protection policies and if needed, create a Managed apps app configuration policy to allow screen capture by configuring the above setting *(Apps > App configuration policies > Create > Managed apps > Step 3 'Settings' under General configuration)*. For more information review, iOS app protection policy settings – Data protection and App configuration policies - Managed apps.

Plan for Change: Implement strong mapping for SCEP and PKCS certificates

With the May 10, 2022, Windows update (KB5014754), changes were made to the Active Directory Kerberos Key Distribution (KDC) behavior in Windows Server 2008 and later versions to mitigate elevation of privilege vulnerabilities associated with certificate spoofing. Windows enforces these changes on **February 11, 2025**.

To prepare for this change, Intune has released the ability to include the security identifier to strongly map SCEP and PKCS certificates. For more information, review the blog: Support tip: Implementing strong mapping in Microsoft Intune certificates .

How does this change affect you or your users?

These changes will affect SCEP and PKCS certificates delivered by Intune for Microsoft Entra hybrid joined users or devices. If a certificate can't be strongly mapped, authentication will be denied. To enable strong mapping:

- SCEP certificates: Add the security identifier to your SCEP profile. We strongly recommend testing with a small group of devices and then slowly rollout updated certificates to minimize disruptions to your users.
- PKCS certificates: Update to the latest version of the Certificate Connector, change the registry key to enable the security identifier, and then restart the connector service. **Important:** Before you modify the registry key, review how to change the registry key and how to back up and restore the registry.

For detailed steps and more guidance, review the Support tip: Implementing strong mapping in Microsoft Intune certificates blog.

How can you prepare?

If you use SCEP or PKCS certificates for Microsoft Entra Hybrid joined users or devices, you'll need to take action before February 11, 2025 to either:

- **(Recommended)** Enable strong mapping by reviewing the steps described in the blog: Support tip: Implementing strong mapping in Microsoft Intune certificates
- Alternatively, if all certificates can't be renewed before February 11, 2025, with the SID included, enable Compatibility mode by adjusting the registry settings as described in KB5014754 . Compatibility mode is valid until September 2025.

Update to the latest Intune App SDK and Intune App Wrapper for Android 15 support

We've recently released new versions of the Intune App SDK and Intune App Wrapping Tool for Android to support Android 15. We recommend upgrading your app to the latest SDK or wrapper versions to ensure applications stay secure and run smoothly.

How does this change affect you or your users?

If you have applications using the Intune App SDK or Intune App Wrapping Tool for Android, it's recommended that you update your app to the latest version to support Android 15.

How can you prepare?

If you choose to build apps targeting Android API 35, you need to adopt the new version of the Intune App SDK for Android (v11.0.0). If you wrapped your app and are targeting API 35, you need to use the new version of the App wrapper (v1.0.4549.6).

> **Note**
>
> As a reminder, while apps must update to the latest SDK if targeting Android 15, apps don't need to update the SDK to run on Android 15.

You should also plan to update your documentation or developer guidance if applicable to include this change in support for the SDK.

Here are the public repositories:

- Intune App SDK for Android
- Intune App Wrapping Tool for Android

Intune moving to support Android 10 and later for user-based management methods in October 2024

In October 2024, Intune supports Android 10 and later for user-based management methods, which includes:

- Android Enterprise personally owned work profile
- Android Enterprise corporate owned work profile
- Android Enterprise fully managed
- Android Open Source Project (AOSP) user-based
- Android device administrator
- App protection policies
- App configuration policies (ACP) for managed apps

Moving forward, we'll end support for one or two versions annually in October until we only support the latest four major versions of Android. You can learn more about this change by reading the blog: Intune moving to support Android 10 and later for user-based management methods in October 2024 .

> ⓘ **Note**
>
> Userless methods of Android device management (Dedicated and AOSP userless) and Microsoft Teams certified Android devices aren't affected by this change.

How does this change affect you or your users?

For user-based management methods (as listed above), Android devices running Android 9 or earlier won't be supported. For devices on unsupported Android OS versions:

- Intune technical support won't be provided.
- Intune won't make changes to address bugs or issues.
- New and existing features aren't guaranteed to work.

While Intune won't prevent enrollment or management of devices on unsupported Android OS versions, functionality isn't guaranteed, and use isn't recommended.

How can you prepare?

Notify your helpdesk, if applicable, about this updated support statement. The following admin options are available to help warn or block users:

- Configure a conditional launch setting for APP with a minimum OS version requirement to warn and/or block users.
- Use a device compliance policy and set the action for noncompliance to send a message to users before marking them as noncompliant.
- Set enrollment restrictions to prevent enrollment on devices running older versions.

For more information, review: Manage operating system versions with Microsoft Intune.

Last updated on 01/12/2026