



Release Notes Android

CONTENTS

1. Ivanti Go 122.0.0 - 126.0.0 for Android Release Notes 3

2. Revision history 4

3. About Ivanti Go for Android 5

4. New features summary 6

5. Support and compatibility 12

6. Resolved issues 16

7. Known issues 17

8. Limitations 19

9. Documentation resources 21

 9.1. Ivanti Neurons for MDM documentation 22

10. Opening a Support Ticket 23

1. Ivanti Go 122.0.0 - 126.0.0 for Android Release Notes

August 2026

These are cumulative release notes. If a page does not list a release, then there is no new associated information for that release.



[New features summary](#)



[Revision history](#)

2. Revision history

Date	Revision
August 26, 2026	Added New features summary , Known issues , Resolved issues , Limitations and Support and compatibility for Go 126 for Android.
April 29, 2026	Added New features summary , Known issues , Resolved issues , Limitations and Support and compatibility for Go 124 for Android.
February 16, 2026	Added New features summary , Known issues , Resolved issues , Limitations and Support and compatibility for Go 122 for Android.

3. About Ivanti Go for Android

Ivanti Go for Android securely connects your Android device to your company network so that you can easily access email and other work resources. Ivanti Go works in conjunction with Ivanti Neurons for MDM supported by your company's IT organization. Please follow the instructions from your IT organization to use this app. Ivanti Go is required to access corporate resources and therefore should not be removed without first consulting your IT organization. Learn about Mobile Device Management (MDM) at *Android Device Management*.

With Ivanti Go, you can:

- Easily get access to corporate resources such as email, calendar and contacts on your Android device.
- Connect automatically to corporate Wi-Fi and VPN networks.
- Discover and install work related applications on your device wherever you are.
- Automatically comply with corporate security policies.
- Locate lost or stolen devices and remotely manage them.

The Sentry Root CA certificate should not be pushed for Android Enterprise devices if the issuer is a publicly trusted Certificate Authority (CA). After certificate renewal, the administrator must edit the Tunnel VPN configuration and save it. The new certificate will then be pushed to the device.

4. New features summary

These are cumulative release notes. If a release does not appear in this section, then there were no associated new features and enhancements.

✓ Ivanti Go 126 for Android - New features summary

- **Enhanced Patch Compliance Messaging:** Users now receive a clear message when device registration fails due to an outdated security patch level. The message reflects the compliance threshold configured in **Device Registration** settings and explains the remediation required to complete registration.
- **Android 17 Day-Zero support:** We introduce day-zero support for Android 17. Ivanti Go for Android is now optimized to operate smoothly on devices running the latest Android 17 OS.
- **Integrated Tunnel Support:** Tunnel functionality is now available directly within the Go Client app through app restriction configuration, providing the same tunneling experience without requiring a standalone Tunnel app. This feature is supported only on newly registered devices.
- **SIM State Change Detection and Reporting:** The Android Go client now detects SIM card insertion/removal events on managed devices.

When a SIM state change is detected:

- The client updates active subscription information in device details/check-in data.
- A Force Device Check (FDC) is triggered so the server receives the updated SIM/subscription state promptly.
- This improves visibility and compliance monitoring for SIM-related changes on managed devices.
- **MGPA to Google Account Device Migration:** In this release, support has been added to migrate existing devices registered with Managed Google Play Accounts (MGPA) to Google accounts by using a BTE token. This enhancement helps organizations transition enrolled devices to the new account model while maintaining uninterrupted device management. A new Key Value Pair is added to enable this feature:

feature.android.bte.enterprise.upgrade.and.device.migration.enabled

Supported Platforms

- Managed Device with Work Profile: Android 12+
- Device Owner: Android 9+
- Profile Owner: Android 9+
- **Settings Access in Single App Kiosk Mode:** Single App Kiosk mode now supports secure access to **Settings** without displaying additional apps or exit options. This allows authorized users to access kiosk settings when needed while the designated kiosk app is in full-screen mode. To access **Settings** in **Single App Kiosk** mode, press and hold both **Volume Up** and **Volume Down** button for 3 seconds. A new KVP is added to enable this feature **feature.android.kiosk.single.app.allow.settings.enabled**.
- **Global Proxy Configuration for Device Traffic:** In this release, administrators can configure a Global Proxy to route device network traffic through a designated proxy server. This setting provides a centralized method for managing proxy configurations across devices.
 - The **Global Proxy** setting is applied as a recommendation, and some applications may choose to bypass or ignore the configured proxy.
 - When configured, the **Global Proxy** setting takes precedence over network-specific proxy settings.
 - This feature is supported only for **Work Managed Device** mode.
- **Update to Target SDK:** The Target SDK has been updated to 36.
- **Support for QR-Based AOSP Device Registration:** Ivanti Go now supports registration of non-AOSP devices in AOSP mode using QR codes generated either through the Provisioner app or from the server.

- **Enhanced Device Registration Block Messages:** Ivanti Go now provides clearer and more informative device registration block messages during enrollment. When device registration is blocked due to configured compliance requirements, users receive detailed messages indicating the specific reason for the block. This enhancement applies to devices enrolled in Device Owner, Profile Owner, and Enhanced Profile Owner modes and covers the following Device Registration Settings:
 - Minimum OS Version
 - Minimum Security Patch Level
 - Manufacturer Whitelist/Blacklist
 - Minimum SafetyNet Certification

These improved messages help users and administrators quickly identify and address registration issues, resulting in a smoother enrollment experience.

- **Google Account Configuration Support in Shared Kiosk Mode:** Ivanti Go now supports configuring Google accounts on devices running in Shared Kiosk mode. This enhancement helps streamline access to Google services in kiosk deployments. Additionally, administrators can configure Gboard (version 16.5 and later) behavior through App Configuration settings, including controls for clipboard access, suggestion strip icons, suggestion removal, and the Settings icon. To ensure the configured settings are applied correctly, administrators must enable the option to clear the Gboard cache in Kiosk Lockdown.

- **Samsung ELM License Activation Bypass Support:** Ivanti Go now supports bypassing Samsung Enterprise License Management (ELM) license activation based on administrator-defined configurations.
- **LEO URL Support in Ivanti Go:** Ivanti Go now supports dynamic LEO URL configuration, allowing administrators to override the default LEO URL when required. This enhancement provides greater flexibility for deployment scenarios by enabling the client to connect to a custom LEO endpoint based on configuration settings, simplifying environment-specific setup and management.
- **Android 17 Day Zero Support for Samsung Devices:** Ivanti Go now provides Day Zero support for Samsung devices running Android 17, enabling organizations to enroll and manage supported Samsung devices as soon as they are upgraded to Android 17. This helps IT administrators adopt the latest Android release without delay while maintaining device management, security, and compliance capabilities.

✓ Ivanti Go 124 for Android - New features summary

- **Enhanced sign-up flow and device enrollment:** Starting from this release, the sign-up and device enrollment experience has been enhanced using Google BTE tokens with Custom DPC on Android 12+ devices.
- **RCS and SMS and MMS Archival Support for Android enterprise:** Ivanti Neurons for MDM now supports automatic archival of Rich Communication Services (RCS), SMS and MMS messages from Google Messages on managed Android enterprise devices.
- **Reporting active SIM subscriptions to Ivanti NMDM:** All active subscriptions available on the device are now reported to Ivanti Neurons for MDM as part of the device details payload.
- **OU attributes support in CSR during Android device enrollment:** Ivanti Go for Android has been enhanced to support populating the **Organizational Unit** (OU) field in the subject of the Certificate Signing Request (CSR) during device enrollment. As part of this update, both the **Organization** (O) and **Organizational Unit** (OU) attributes are now submitted as required fields in the CSR to the DoD approved Certificate Authority.
- **On Demand App cache clearing from N MDM console:** Ivanti Go for Android has been enhanced to support on demand clearing of application caches initiated directly from the Ivanti Neurons for MDM console. This enhancement applies to all apps installed on the device, including both corporate or enterprise applications and third party apps.
- **Custom ticketing portal link in Support tab:** Administrators can now configure a custom ticketing portal URL within the application. This URL is displayed in the **Support** tab, allowing end users to directly access the configured portal for submitting support tickets using **Raise a Support Ticket**.
- **Smishing protection enhancement:** In Ivanti Go for Android, Smishing protection can now be managed through the Ivanti Portal.

Disabling Smishing protection causes the app to restart.

✓ Ivanti Go 122 for Android - New features summary

- **Enhanced eSIM configuration support:** Devices can now install eSIM configurations across all supported provisioning modes:
 - Work Profile
 - Work Profile on Company Owned Device
 - Work Managed Device

Auto Enable eSIM

A new **Auto Enable** functionality is now available for eSIM configurations, allowing the eSIM profile to activate automatically after installation.

This functionality is supported only in Work Profile on Company Owned Device and Work Managed Device modes.

Automatic eSIM Profile Removal on Configuration Uninstall

When an eSIM configuration is uninstalled from the device, the associated **eSIM profile** is automatically deleted from the devices.

Enhanced wipe settings

The option to retain data plans during device operations is now available on Android 15 and later.

- If the checkbox is unchecked, the system will erase all eSIM data plans from the device.
- If the checkbox is checked, the device's existing data plans are retained.
- **Enhanced Terms of Service format support:** Ivanti Go for Android extended support for displaying the Terms of Service in HTML format, in addition to the existing plain text format.
- **New Support Tab for enhanced user assistance:** A new **Support** tab has been added to the client menu, giving end users quick access to essential help resources. This tab provides step by step instructions, support contact information, useful reference links, and additional support details.
- **New Logout button for Kiosk users:** A **Logout** button has been added to the Kiosk home screen, making it easier and more intuitive for kiosk users to securely log out their session.
- **New Lockdown Policy for AppFunctions:** A new lockdown option has been introduced to enhance control over the AppFunctions policy.

The lockdown includes three configurable states:

- Not Controlled
- Disabled
- Disabled for Cross Profile

AppFunctions policy is supported in Work Profile on Company Owned Device, Work Managed Device, and Work Profile.

- **Enhanced EID retrieval for Android devices:** Support has been added in Ivanti Go for Android to fetch EID values on Android devices running Android 13 and later. The retrieval behavior varies based on the device ownership mode:
 - **Work Managed Device mode:** EID values are retrieved automatically without user interaction.
 - **Work Profile and Work Profile on Company Owned Device modes:** EID values are retrieved only when a request command is issued from the server.
- **Update Lookout SDK to Version 4.2.5.193:** The Lookout SDK has been updated to 4.2.5.193.
- **Support for Samsung Knox SDK 3.12:** Ivanti Go for Android now integrates with Samsung Knox SDK version 3.12.

- **Easy Access to End User License Agreement (EULA):** Users can now view the End User License Agreement (EULA) directly in Ivanti Go for Android. The EULA can be accessed by navigating to: **Settings > About**.
- **Enhancement in device registration:** Ivanti Go for Android has been enhanced to restrict device registration based on the supported enrollment type. This enhancement allows only with the following enrollment methods:
 - Samsung Knox Mobile Enrollment (KME)
 - Google Zero-Touch Enrollment

5. Support and compatibility

These are cumulative release notes. If a release notes does not appear in this section, then the support and compatibility values from the nearest listed older release apply to the missing release.

▼ Ivanti Go 126.0 for Android - Support and compatibility

Product	Supported versions	Compatible versions
Ivanti Neurons for MDM	R126 and R125	R125, R123, R122, and R121,
Android	9, 10, 11, 12, 13, 14, 15, 16 and 17	

Supported languages

The following languages and locales are supported in this version:

- Arabic
- Catalan
- Chinese (Simplified)
- Chinese (Traditional)
- Croatian
- Dutch
- English
- Finnish
- French (France)
- German (Germany)
- Hungarian
- Italian (Italy)
- Japanese
- Korean
- Portuguese (Brazil)
- Spanish (Latin America)
- Spanish (Spain)
- Swedish

▼ Ivanti Go 124.0 for Android - Support and compatibility

Product	Supported versions	Compatible versions
Ivanti Neurons for MDM	R124 and R123	R122, R121, R120, and R119
Android	9, 10, 11, 12, 13, 14, 15 and 16	

Supported languages

The following languages and locales are supported in this version:

- Arabic
- Catalan
- Chinese (Simplified)
- Chinese (Traditional)
- Croatian
- Dutch
- English
- Finnish
- French (France)
- German (Germany)
- Hungarian
- Italian (Italy)
- Japanese
- Korean
- Portuguese (Brazil)
- Spanish (Latin America)
- Spanish (Spain)
- Swedish

▼ Ivanti Go 122.0 for Android - Support and compatibility

Product	Supported versions	Compatible versions
Ivanti Neurons for MDM	R122 and R121	R120, R119, and R118
Android	9, 10, 11, 12, 13, 14, 15 and 16	

Supported languages

The following languages and locales are supported in this version:

- Arabic
- Catalan
- Chinese (Simplified)
- Chinese (Traditional)
- Croatian
- Dutch
- English
- Finnish
- French (France)
- German (Germany)
- Hungarian
- Italian (Italy)
- Japanese
- Korean
- Portuguese (Brazil)
- Spanish (Latin America)
- Spanish (Spain)
- Swedish

Support policy

Ivanti defines supported and compatible as follows:

Term	Definition
Supported product versions	The functionality of the product and version with currently supported releases was systematically tested as part of the current release and, therefore, will be supported.
Compatible product versions	The functionality of the product and version with currently supported releases has not been systematically tested as part of the current release, and therefore not supported. Based on previous testing (if applicable), the product and version is expected to function with currently supported releases.

6. Resolved issues

These are cumulative release notes. If a release does not appear in this section, then there were no associated resolved issues.

✓ **Ivanti Go 126.0 for Android - Resolved issue**

- **1934448:** This release includes maintenance updates and stability improvements.

✓ **Ivanti Go 122.0 for Android - Resolved issue**

- **1411442:** The Zimperium V5 console cannot detect the following threats even after activating them:
 - Active ADB Session
 - Location Permission

7. Known issues

These are cumulative release notes. If a release does not appear in this section, then there were no associated known issues.

✓ Ivanti Go 126 for Android - Known issue

- **1591019:** When a device is retired from **Work Profile on Company Owned Device** mode and subsequently registered in **Work Profile** mode, any app that was previously whitelisted during **Work Profile on Company Owned Device** mode registration remains pinned in the Play Store.
- **1729772:** When the configuration is undistributed, the eSIM profile is not deleted from the device. This behavior is observed only on Android 16 in Work Profile and Work Profile on Company Owned Device modes.
- **1909820:** On Samsung devices running Android 13, the accessibility settings flow may not function as expected when the device is in kiosk mode. This occurs if com.android.settings and com.samsung.accessibility are not included in the kiosk whitelist on the server.
- **1908370:** During account upgrade using an enrollment token, the **Skip** option may still appear on the Google authentication screen for some devices when account migration is configured.
- **1920265:** Samsung Pass pop-ups may appear on devices in Lockdown & Kiosk mode if the associated system apps are not disabled. To prevent this, administrators must add the following packages under the **Disable system** app section:
 - com.samsung.android.samsungpassautofill
 - com.samsung.android.samsungpass
 - com.samsung.android.authfw
- **1920268:** While configuring a Gmail account on Samsung EAT devices operating in Kiosk mode, Google Services may crash unexpectedly. As a result, users may be able to exit the Kiosk environment during the account configuration process.
- **1937845:** Anti-phishing status updates may not be displayed immediately on all devices. While some devices reflect the updated status right away, others may experience a delay before the status is refreshed. In certain cases, users may need to minimize and reopen the app to view the latest anti-phishing status.
- **1966536:** On Android 9 devices, the **Skip** option may not appear on the Google authentication screen during device enrollment when the **Authenticate Using Google** feature is enabled through the Google Admin Console. As a result, users may be required to complete Google authentication before proceeding with enrollment.

✓ Ivanti Go 124 for Android - Known issue

- **1713003:** On Samsung devices with dual SIM capability, fetching the Embedded Identity Document (EID) is not supported.
- **1777426:** During device provisioning, the AMAPI SDK may encounter a timeout while preparing the environment. If this step fails, the device does not complete the provisioning process.

Workaround: You can retry the provisioning operation.

✓ Ivanti Go 122 for Android - Known issue

- **1726207:** After a fresh device enrollment, the initial EID request may fail with a timeout error. The device may need additional time to complete these updates before the EID can be retrieved successfully.

Workaround: IT administrators can send the request EID server command again to retry the process once the device has completed its background initialization.

8. Limitations

These are cumulative release notes. If a release does not appear in this section, then there were no associated limitations.

✓ Ivanti Go 126 for Android - Limitation

- **1732063:** The application cannot detect a manageable eSIM and always returns an error to the server, preventing eSIM profile removal upon configuration undistribution. This behaviour is observed on Samsung devices running Android 15 in Work Profile and Work Profile on Company Owned Device modes.
- **1955924:** The Integrated Tunnel option is not supported on the Ivanti Go client when devices are enrolled in COPE (Corporate-Owned, Personally Enabled) mode. As a result, the Integrated Tunnel option is not enabled or available for use on COPE-managed devices.
- **1873590:** On some devices, Google account enrollment may fail if Google Play Services is outdated or not functioning correctly. Administrators should ensure that Google Play Services is updated and operating properly before attempting to add a Google account. If the issue occurs, updating and refreshing Google Play Services, followed by a device restart, may be required before retrying the enrollment process.

Workaround

If Google account setup fails, perform the following steps:

- Go to **Settings > Lock screen and security > Other security settings > Device admin apps > Find My Device > Disable**.
- Go to **Settings > Apps > Google Play Services > More options > Uninstall updates**.
- Update Google Play Services:
 - **Settings > Google > More > Help & Feedback > More > View in Google Play Store > Update**, or Go to Chrome.
Search **Google Play Services**.
Install the latest update from the Google Play Store.
- Go to **Settings > Application > Google Play Services > Storage > Manage Storage > Clear cache**, clear all data.
- Restart Device.
- Wait at least 30 minutes, reboot the device again, and retry adding the Google account.

Ensure the device is connected to a stable network throughout the process.

✓ Ivanti Go 124 for Android - Limitation

- **1591017:** Suspended apps in the work profile are sometimes displayed as greyed out, as expected. However, in rare cases, these same apps may not appear as greyed out on the home screen.

✓ Ivanti Go 122 for Android - Limitation

- **1685871:** The behavior is due to ongoing Google vendor issue (status: *In progress*).

Users should avoid enabling 16KB page support until the vendor issue is fully resolved.

9. Documentation resources

Product documentation is available on the [Ivanti documentation website](#). You can access the Ivanti Ivanti Go 122.0.0 - 126.0.0 for Android Release Notes directly at [this link](#).

To use the documentation:

1. Navigate to the [Ivanti documentation website](#).
2. Optionally, select a product category and language.
3. Enter a search term, or scroll down to find the required product.
4. Select a product from the results.
5. Click the associated documentation links.

9.1. Ivanti Neurons for MDM documentation

- [Ivanti Neurons for MDM Release Notes](#)

Contains the following release-specific information: new feature summary, support and compatibility, known and resolved issues, and limitations.

- [Ivanti Neurons for MDM Administrator Guide](#)

Contains information for getting started, registering users and devices, adding, configuring, and managing apps, creating and managing configurations and policies for apps, security, certificates, device and user licenses, package licenses, and license upgrades, and device use self-service portal for managing devices.

Information about Email+, Web@Work, and Docs@Work are covered in the guides for the apps.

Information about Sentry, AppConnect, and Access are covered in related product guides. AppTunnel, ActiveSync, and Zero Sign-on information appears in appropriate areas of various product guides.

- [Ivanti Neurons for MDM Connector Installation Guide](#)

Ivanti Neurons for MDM Connector is required to set up access from Ivanti Neurons for MDM to corporate resources, such as an LDAP server or a Certificate Authority (CA). Contains information pertaining to requirements, installing and configuring the Connector Open Virtual Appliance (OVA), deploying Connector in AWS, installing the Connector ISO package, using the Configuration Wizard, and maintenance and troubleshooting.

- [Ivanti Neurons for MDM Customer Integration API Guide](#)

Describes how to integrate your environment with Ivanti Neurons for MDM using the public Integration API calls. If the guide does not include a call, then Ivanti does not support that call for public use.

- [Event Notification Service and Common Platform Services API Guide](#)

Describes how to use the Event Notification Service and Common Platform Services (CPS) API with Ivanti Neurons for MDM and Core.

- [Core to Ivanti Neurons for MDM Migration Portal User Guide](#)

Describes the steps to migrate from Core to Ivanti Neurons for MDM using the Low User Impact Migration Portal, a cloud-based service for migrating devices from Core to Ivanti Neurons for MDM.

- [Splunk Enterprise app for Ivanti Neurons for MDM Release Notes](#)

Contains the following release-specific information: new feature summary, support and compatibility, upgrade notes, known and resolved issues, and limitations.

- [Splunk Enterprise app for Ivanti Neurons for MDM User Guide](#)

Describes how to set up and use the Splunk Enterprise app for Ivanti Neurons for MDM.

- [ServiceNow Integrator Update Set Guide](#)

Describes how to set up and use the ServiceNow Integrator Update Set for Ivanti Neurons for MDM.

The preceding links were the most recent at the time of publication. To ensure that you are getting the latest Ivanti Neurons for MDM documentation visit [this link](#).

10. Opening a Support Ticket