



Release Notes

iOS

CONTENTS

Ivanti Go 104 - 126.0.4 for iOS Release Notes	3
Revision history	4
About Ivanti Go for iOS	5
Mobile Threat Defense features	6
New features summary	7
Support and compatibility	13
Resolved issues	16
Known issues	17
Limitations	18
Third Party Attributes	19
Documentation resources	20
Ivanti Go for iOS documentation	21
Apps@Work	22
Common Threat Scenarios Detected by MTD	24
Compliance Messages	25
Data Management	27
Device Status	28
Features and Homescreen Guide	29
Ivanti Go for iOS documentation	30
Ivanti Tunnel	31
Additional configurations using key-value-pairs	32
Apps@Work	34
Common Threat Scenarios Detected by MTD	36
Compliance Messages	37
Data Management	39
Device Status	40
Features and Homescreen Guide	41
Ivanti Tunnel	42
Notifications	43
Privacy and Data Separation	44
Privacy Settings	45
Self-Service Return to Service	46
Security Features	48
Settings	49
Support Tab	51
MTD functionality	52
Mobile Threat Defense (MTD)	53
Actions after Detecting a Compliance Violation	54
Notifications	55
Privacy and Data Separation	56
Privacy Settings	57
Self-Service Return to Service	58
Security Features	60
Settings	61
Support Tab	63
MTD functionality	64
Mobile Threat Defense (MTD)	65
Actions after Detecting a Compliance Violation	66

Ivanti Go 104 - 126.0.4 for iOS 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](#)

Revision history

Date	Revision
August 07, 2026	Updated for Ivanti Go 126.0.4 for iOS.
July 29, 2026	Updated for Ivanti Go 126.0.2 for iOS.
July 23, 2026	Updated for Ivanti Go 126.0.0 for iOS.
April 21, 2026	Updated for Ivanti Go 124.0.0 for iOS.
January 21, 2026	Updated for Ivanti Go 122.0.0 for iOS.
November 10, 2025	Updated for Ivanti Go 120.0.1 for iOS.
October 21, 2025	Updated for Ivanti Go 120 for iOS.
September 24, 2025	Updated for Ivanti Go 118.0.1 for iOS.
July 23, 2025	Updated for Ivanti Go 118 for iOS.
April 23, 2025	Updated for Ivanti Go 116 for iOS.
February 26, 2025	Updated for Ivanti Go 112.0.1 for iOS.
January 27, 2025	Updated for Ivanti Go 112 for iOS.
November 6, 2024	Updated for Ivanti Go 108 for iOS.
October 3, 2024	Updated for Ivanti Go 106 for iOS.
July 4, 2024	Updated for Ivanti Go 104 for iOS.

About Ivanti Go for iOS

Ivanti Go for iOS securely connects your iOS device to your company network, and lets you do the following:

- Easily access to corporate resources like email, calendar, and contacts on your iOS 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.

Ivanti Go works with Ivanti Neurons for MDM supported by your 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. For more information about Mobile Device Management (MDM), see

<https://www.ivanti.com/company/history/mobileiron?miredirect>.

Ivanti Go upgrade information

After upgrading to Ivanti Go 120 or later, if an AppConnect passcode is required, as a user you must set a new passcode when they first launch Ivanti Go or AppConnect app. If the passcode policy changes and Ivanti Go is upgraded, users are prompted to set a new passcode or biometric at launch and may be prompted again later for authentication.

Mobile Threat Defense features

MTD is a built-in security feature available in Ivanti Go app. MTD continuously monitors your device for cyber threats that could affect both work and personal use. MTD monitors risks and vulnerabilities, then guides you to take correct actions - keeping your device, your data, and organizations resources secure.

Mobile Threat Defense (MTD) protects managed devices from mobile threats and vulnerabilities affecting device, network, and applications. For information on MTD-related features, as applicable for the current release, see the Mobile Threat Defense Solution Guide for your platform, available under the MOBILE THREAT DEFENSE section on the [Ivanti Product Documentation page](#).

Each version of the MTD guide contains all Mobile Threat Defense features that are currently fully tested and available for use on both server and client environments. Because of the gap between server and client releases, new versions of the MTD guide are made available with the final release in the series when the features are fully functional

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 126.0.4 for iOS

- **New KVP added for control Certificate Renewal behavior:** Ivanti Go now provides additional Managed App Configuration Key Value Pairs (KVPs) to give administrators greater control over client certificate renewal. Administrators can disable automatic certificate renewal and optionally expose a **Renew Client Certificate** option in the **Troubleshoot** menu, enabling users to manually renew certificates when required.

The Managed App Configurations KVPs used to control certificate renewal behavior in the app are as follows:

- **AutoCertRenewalDisabled**
- **TroubleshootCertRenewalEnabled**

For more information, see *iOS Go Advanced Features* in the *Neurons for MDM Administrator Guide*.

✓ Ivanti Go 126.0.0 for iOS

- **Managed App Distribution Framework Support:** Ivanti Go for iOS now supports Apple's ManagedAppDistribution framework, enabling managed app discovery and installation through Declarative Device Management (DDM) on supported iOS devices. The framework provides a native app catalog experience, including app listing, app details, category-based browsing, search, and app installation capabilities directly within the Ivanti Go client. This implementation leverages Apple's built-in framework for managed app distribution and delivers real-time app status updates, streamlined app management, and a unified app catalog experience. When enabled by the server, app management transitions to Declarative Device Management (DDM) for managed public and VPP applications on supported iOS versions as part of the initial phase. Apps@Work is updated with this framework when customers enable DDM app management on the device.
- **Support for Lookout SDK 4.2.8:** Lookout SDK version 4.2.8 is now supported with this release.
- **Restrict Log Sharing to Approved Email Clients:** In this release, Ivanti Go introduces a new managed configuration key that allows administrators to restrict log sharing to an approved email client. When enabled, device and application logs can only be shared through the configured email app, helping organizations control how log data leaves managed devices. Logs are automatically attached when supported by the selected email client, while other clients use a guided attachment workflow. This enhancement improves security by preventing logs from being shared through unauthorized apps or destinations. The automated attachment of logs is supported on Native Email and Email+.
- **Integrated Tunnel Revamped:** Enhanced Tunnel User Interface in Ivanti Go.
- **Tunnel Visibility Based on Configuration:** In this release, Ivanti Go now display Tunnel functionality when Tunnel VPN configuration is explicitly distributed to the iOS client. If no Tunnel configuration is assigned, Tunnel-related options remain hidden, reducing user confusion in environments where Tunnel is not in use. Additionally, Tunnel functionality is automatically removed from the client when the associated configuration is withdrawn, ensuring that only relevant features are presented to users.
- **Device Check-In Status Verification:** Ivanti Go now provides immediate feedback when users manually select Check for Updates. After the device successfully checks in with the server, the app displays a confirmation notification, giving users clear visibility that the check-in was completed successfully. A pop up message is displayed when users swipe down to refresh, Tap on '**Check for updates** and FDC from **My Devices**. This enhancement improves the user experience by providing real-time status confirmation and reducing uncertainty about the outcome of the check-in operation.
- **Updated User Interface for Status and Notification Screens :** The **Notification, Device Status, and Threat Defense screens** is updated with an enhanced table view design to provide a more modern and consistent user experience. The refreshed interface improves readability, navigation, and overall usability, making it easier for users to view and access important device and security information.
- **Customize Email and Browser Apps for Support:** In this release, Ivanti Go for iOS introduces KVPs that allows administrators to customize the default email and browser applications used by the **Support** tab and log-sharing workflows. For more information, see **iOS Go Advanced Features** in the *Neurons for MDM Administrator Guide*.
 - **default_browser**
 - **allow_browser_fallback**
 - **default_email**
 - **allow_email_fallback**
 - **restrict_log_sharing_to_email**

✓ Ivanti Go 124.0.0 for iOS

- **Return to Service enhancement:** When **Return to Service** is enabled, the **Return to Service** button is now available on the **Home Screen** for quicker access.
- **Support for Lookout SDK 4.2.6:** Lookout SDK version 4.2.6 is now supported with this release.
- **Go for iOS support deprecation (iOS 16.x):** Starting from this release, Ivanti Go for iOS support has been deprecated on devices running iOS 16.x.
- **Enhanced device check-in on network changes:** Device management has been enhanced with improved controls to ensure timely device check-ins when network status changes. When a device switches between Wi-Fi and cellular networks, a force check-in is automatically triggered.
- **Improved App update status display:** When an update is available, the **Featured** tab now displays **Update** instead of **Install**.

✓ Ivanti Go 122.0.0 for iOS

- **Support Ticketing Integration in Ivanti Go:** Ivanti Go for iOS now introduces a new **Support Ticketing System URL** feature designed to make it easier for users to report issues directly from the app with a single tap.
- **Integrated Ivanti Tunnel support in Ivanti Go (iOS):** Ivanti Go for iOS now includes Ivanti Tunnel capabilities, fully supporting all features previously available in the standalone Ivanti Tunnel app. For more information, see [Ivanti Tunnel for iOS Guide](#).
- **Support for Liquid Glass:** Ivanti Go for iOS now includes full support for Liquid Glass UI design language for iOS.
- **Upgrade to Zimperium SDK:** Starting from this release, we support integration with the Zimperium SDK version 5.8.53.
- **Revamped client screens:** Starting from this release, Ivanti Go for iOS introduces a fresh client interface designed to enhance the user experience.

✓ Ivanti Go 120.0.0 for iOS

- **Smishing protection support:** We now support Smishing protection to safeguard users from SMS-based phishing attacks. Administrators can easily enable and manage Smishing protection by configuring relevant settings within the Lookout console.
- **Simplified device registration process:** Starting with this release, you can access the browser within the Ivanti Go for iOS application when you register a new device, instead of redirecting the registration process to the default browser of the device.
- **Support for Lookout SDK 4.2.3:** Lookout SDK version 4.2.3 is now supported with this release.
- **iOS Developer Mode Threat Detection:** Lookout now supports the detection of iOS devices with Developer Mode enabled. This enhancement helps prevent potential security risks associated with Developer Mode, such as unauthorized app installations or bypassing built-in security controls.
- **Passkey authentication support:** Starting with this release, Ivanti Go for iOS supports Passkey authentication.

✓ Ivanti Go 118.0.1 for iOS

- **iOS 26 Support:** Ivanti Go for iOS now supports iOS 26.

✓ Ivanti Go 118.0.0 for iOS

- **Notification Icon Relocation:** The notification icon on the client home screen has been moved to the upper right corner.
- **Customizable Out of Compliance Messages:** Admins can now customize **Out of Compliance** messages by uploading a custom plist file to the server. Once uploaded, these messages can be pushed directly to devices, allowing for tailored communication and improved compliance management across your organization. For more information, see [Using Apple Managed App Configuration](#).
- **Customizable Support Tab:** A new Support tab is now available in the Ivanti app, enabling admins to display support contact details and useful links to end-users. This tab can be customized and set as the home screen with the following fields:
 - **Tab Name:** Maximum 10 characters (default: "Support")
 - **Contact Name:** Maximum 40 characters
 - **Support Phone:** Maximum 20 characters
 - **Support Email:** Maximum 40 characters (valid email format required)
 - **Website Name:** Maximum 40 characters
 - **Website URL:** Maximum 150 characters (must be a valid https:// link)
 - **Additional Info:** Maximum 120 characters

Admins can now configure these fields using the server, with field validation enforced for accuracy.

Clients display the configured tab and links on their app, enabling them to conveniently contact support or visit the [support site](#) for assistance.

✓ Ivanti Go 116.0.0 for iOS

- **Support for Lookout SDK 4.1.17:** Lookout SDK version 4.1.17 is now supported with this release.
- **Enhanced security for sensitive screens:** The **Registration** and **SAML Authentication** screens are now protected by default against screen shots, screen recording, and screen sharing. On managed devices, administrators can selectively disable this protection for the SAML Authentication screen using the key-value pair:
SCREENSHOT_PROTECTION_DISABLED = True
- **Upgrade to Zimperium SDK:** Starting from this release, we now integrate with the Zimperium SDK version 5.6.37.
- **iOS 15 deprecation:** Starting with this release, Go for iOS no longer supports iOS 15.
- **Note for Former App Station users:** Ivanti recommends transitioning to the Ivanti Go Client for iOS. Ivanti Go Client provides a comprehensive MAM solution that includes an in-app App Catalog and Web clip functionality. For more information, see [MAM-Only](#).

Migration Guidance

Ivanti strongly encourages App Station customers to begin planning and executing their transition to the Go Client-based MAM-Only solution. For step-by-step migration assistance, see the following resources:

- [Ivanti MAM-Only Solution](#)
- [App Catalog Configuration in Go Client](#)
- [Create a Web Clip Configuration](#)

If you have questions or need migration assistance, please contact [Ivanti Support](#) or your Customer Success Manager.

✓ Ivanti Go 112.0.0 for iOS

- **Enhancement for Ivanti N-MDM Azure:** Ivanti N-MDM now supports Azure Device Compliance in both GCC High and DoD environments. This enhancement ensures that organizations operating in these specialized environments can continue to leverage Ivanti N-MDM for secure and compliant device management.
- **Change in Ivanti N-MDM user experience:** The **Re-enroll** button has been removed from devices enrolled through Apple's Device Enrollment Program (DEP), streamlining the user interface and device management process.
- **Support for Migration from Zimperium V4 to V5:** The migration from Zimperium V4 to V5 is now supported using [Ivanti Support](#) requests. The support team helps you migrate your existing devices from the Zimperium V4 console to V5. This method includes recreating admin users, groups, policies, and other V5 configurations for your device groups.
- **Reinstall button for Integrated AppCatalog:** Ivanti Go for iOS has introduced a **Reinstall** button on the Integrated App Catalog device. This button allows you to reinstall the app immediately when necessary.
- **Enhancement to deep link:** We introduce a new deep link feature that allows you to create custom webclips that launch the **AppCatalog** in Ivanti Go for iOS. This feature launches an integrated app catalogue, allowing you to open apps directly from the following link.
 - DeepLink URL to show AppCatalog page: `mobileirongo://deeplink/navigation?screen=app_catalog`
 - DeepLink URL to show open specific app details: `mobileirongo://deeplink/navigation?screen=app_details&bundle_id=<bundle_id>`

✓ Ivanti Go 108.0.0 for iOS

- **Support for Zimperium v5 Console:** For the new customers, Ivanti Go for iOS now supports the new Zimperium v5 console.
- **Update to Go for iOS user interface for Zimperium Dynamic Threat detection:** The Go for iOS Threat Defense user interface is redesigned to support dynamic threats detected by the server. The threat defense card displays count based on severity, while the Threats Defense page lists all types of threats, sorted based on their severity.
- **Dynamic threat detection enhancements:** Starting with this release, you can filter low-severity threats using Zimperium threat object values. The Go for iOS now displays threat alert strings from the Threat object, and the server will remove the custom text enabled button.

✓ Ivanti Go 106.0.0 for iOS

- **Support for iOS 18:** Ivanti Go for iOS now supports iOS version 18.
- **New Return to Service option:** The Ivanti Go for iOS now includes an **Enable Return to Service** option which allows the device to automatically re-enroll once data is wiped, reducing the need to manually re-enroll the device after a wipe.

If you want the **Enable Return to Service** option to be visible to end users, you must set a new Key-Value Pair (KVP) setting, **ReturntoService = true**, in the managed app configurations.

Support to collect Ivanti Tunnel logs: Ivanti Go for iOS now collects the Ivanti Tunnel logs from the application. Administrators can view these logs from the Ivanti Neurons for MDM.

✓ Ivanti Go 104.0.0 for iOS

- **Updated partner SDK version:** Starting from this release, Ivanti Go 104 for iOS is now updated to partner SDK versions from 5.3.17 to 5.4.16.
- **Remove filtering for threats:** Remove the filtering based on the availability of local actions to display all threats for Android and iOS.
- **Catalan language support:** Starting from this release, Ivanti Go 104 for iOS now supports Catalan language.

Support and compatibility

These are cumulative release notes. If a release 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 126.0.0 for iOS

Supported components

Table 1. SUPPORTED COMPONENTS

Product	Supported	Compatible
Ivanti Neurons for MDM	124,125	123
iOS	iOS 17.x to iOS 18.x and iOS 26.x	

Supported languages

The following languages and locales are supported for this release:

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

▼ Ivanti Go 124.0.0 for iOS

Supported components

Table 2. SUPPORTED COMPONENTS

Product	Supported	Compatible
Ivanti Neurons for MDM	123,122	121
iOS	iOS 17.x to iOS 18.x and iOS 26.x	

Supported languages

The following languages and locales are supported for this release:

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

Support policy

Table 3. DEFINITIONS FOR SUPPORTED AND COMPATIBLE

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.

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 126.0.4 for iOS

- **1970371:** Previously, device check-in failed after upgrading to Ivanti Go versions 126.0.0 or 126.0.1. This issue has been fixed.

✓ Ivanti Go 126.0.2 for iOS

- **1968820:** Previously, the **Login** and **Retry** prompt was displayed due to an iOS Go client check-in failure. This issue has been fixed.

✓ Ivanti Go 126.0.1 for iOS

- **1969722:** Previously, AppConnect applications could fail to authorize correctly in Ivanti Go for iOS 126.0.0. This issue has been fixed.

✓ Ivanti Go 120.0.1 for iOS

- **1699857:** Previously, the Jailbreak Detection Guard can trigger a tamper action on some devices that were not jailbroken, especially following an update to iOS 26. This issue is now resolved.

✓ Ivanti Go 112.0.1 for iOS

- **1526713:** The jailbreak detection was incorrectly triggered when the device was running out of storage, which is now fixed in this release.
- **1516933:** Previously, Ivanti Go for iOS would erroneously stop while accessing the integrated Ivanti Apps@Work, this is fixed now.

✓ Ivanti Go 112.0.0 for iOS

- **1465094:** **New Threats Found** text was previously truncated with the device border screen, which is now fixed in this release.

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 120.0.0 for iOS

- **1699857:** The Jailbreak Detection Guard may trigger a tamper action on some devices that are not jailbroken. This trigger appears after updating to iOS 26, but it usually resolves on its own after some time.

✓ Ivanti Go 118.0.1 for iOS

- **1635806:** On iPadOS 26, when Ivanti Go for iOS app is resized, the keyboard may appear unexpectedly within the application interface.
- **1635901:** On iPadOS 26, the **Enter full screen** option may not function correctly for resized Ivanti Go for iOS app screen size. You may experience issues when attempting to switch to full screen mode in these scenarios.

✓ Ivanti Go 118.0.0 for iOS

- **1621753:** A customized message for **MDM_DISABLED** cannot be displayed when the profile is disabled. In this state, the client is treated as an unmanaged app and is unable to display the customized message.

✓ Ivanti Go 108.0.0 for iOS

- **1463863:** Ivanti Go for iOS erroneously duplicates a threat notification.

Limitations

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

✓ **Ivanti Go 108.0.0 for iOS**

- **1382747:** Non-App Store Signer (NASS) threats are not detected on iOS 17.5.x devices.

✓ **Ivanti Go 106.0.0 for iOS**

- **1382747:** Non-App Store Signer (NASS) threats are not detected on iOS 17.5.x devices.

✓ **Ivanti Go 104.0.0 for iOS**

- **1382747:** Non-App Store Signer (NASS) threats are not detected on iOS 17.5.x devices.

Third Party Attributes

Ivanti Go for iOS includes components developed by third parties. You can view the list .

 [here](#)



Documentation resources

Product documentation is available on the [Ivanti documentation website](https://help.ivanti.com), help.ivanti.com.

Procedure:

1. Navigate to the [Ivanti documentation website](https://help.ivanti.com).
2. (Optional) select a product category and language.
3. Enter a search term.
4. Select a product from the results.
5. Click the associated documentation links.

Ivanti Go for iOS documentation

The following is a complete list of documentation for this product. However, the list of documents updated for specific versions will vary, depending on release requirements. Therefore, you might encounter documents from previous releases that still apply to the current release.

- [Go for iOS Release Notes](#)

Summary of new features, support and compatibility, known and resolved issues, and limitations.

- [Go for iOS User Guide](#)

Ivanti Go is a mobile application designed to work with the Ivanti Neurons for MDM, which supports iOS and Android platforms. It helps organizations securely manage and enable mobile device access to company resources.

Apps@Work

Apps@Work is your organization's secure app store that provides easy access to all the work-related applications you need. Instead of browsing public app stores such as the Apple App Store, Apps@Work offers a curated catalog of apps that your IT team has approved for your role. Every app listed here has been reviewed for security, relevance, and usability, ensuring you can trust the tools you install.

When you open Apps@Work, you can explore the catalog like other app store. You can:

- Browse for work related apps.
- View descriptions and screenshots that explain about an app and its benefits.
- Check installation status while using Apps@Work clearly shows which apps are already installed on your device.

Some apps may be:

- Required for your job,
- Recommended to support productivity, or
- Optional tools you can choose to install as needed.

This helps you easily identify what's available and what may need to be updated.

Installing Apps

Installing apps through Apps@Work is quick and effortless.

Simply tap an app to begin installation—no additional configuration, setup steps, or technical knowledge are required.

In many cases:

- Apps install automatically, and
- Updates are applied without manual action, ensuring you always have the latest, secure versions.

This automatic maintenance keeps your device secure and minimizes interruptions to your workflow.

Privacy and Security

Apps@Work is designed with your privacy in mind. It manages only work-related apps and does not access your personal apps or personal data.

Your personal space on the device remains completely private.

This separation ensures:

- Your organization can safely deploy work tools.
- You retain full control over your personal applications and information.

Benefits of Apps@Work

Apps@Work provides a convenient, centralized place to discover and install all your work apps. It helps you:

- Save time by avoiding public app store searches.
- Reduce confusion with a curated, role specific app catalog.

- Stay secure with verified, IT approved apps.
- Remain productive with seamless updates.

The Apps@Work screen includes the following tabs at the top:

- **Featured:** Highlights recommended apps
- **All apps:** Displays the complete list of apps available to the user
- **Categories:** Groups apps by functional category

For more information, see [iOS Apps@Work](#).

Common Threat Scenarios Detected by MTD

The common threat scenarios that mobile Threat Defense (MTD) detects are as follows:

- **Malware and Risky Apps:** If the apps are downloaded from unofficial app stores, or those requesting excessive permissions, then they are flagged as risk. MTD alerts you and guides you to uninstall such apps.
- **OS Vulnerabilities:** If your operating system is outdated or known vulnerable, you will receive a compliance alert directing you to update your device software.
- **Jailbroken or Rooted Device:** If your device is modified, reducing security, MTD blocks access to organization data until restored.
- **Unsafe Wi-Fi Networks:** If you connect to public or untrusted networks, MTD enables for threats such as "man-in-the-middle" attacks. MTD prompts you to disconnect or switch networks.
- **Phishing & Network Attacks:** If there are some advanced MTD features, they can detect attempts to steal credentials or intercept communications on untrusted networks.
- **Configuration Issues:** If the weak security settings, such as disabled encryption or weak passwords, are present, then the issue is flagged.

Compliance Messages

Compliance messages in Ivanti Go for iOS appear because your organization enforces specific security rules and standards to protect sensitive business data. These policies apply to both corporate-owned and personal - Bring Your Own Device (BYOD) devices to ensure they remain secure, trustworthy, and eligible for accessing organizations resources and apps. You need to fulfill these compliance requirements to help safeguard business information and maintain a secure work environment.

Managing Rule Ownership and Responsibilities

Your organization's IT Administrator defines security policies in the Ivanti platform. These policies determine the following requirements that the devices must meet:

- Mandatory pass codes and screen locks
- Device encryption
- Latest OS or software updates
- Secure Wi-Fi usage
- No risky apps or configurations (examples: Malware, Jailbreaking)
- Mobile Threat Defense (MTD) actions
- Every organization's standards may differ based on industry regulations, security needs, and risk profiles.

Common Compliance Messages

The following list contains compliance messages that will appear on the devices:

- **Passcode Required:** "Please set a device passcode to access organization resources."
- **Encryption Needed:** "Enable encryption to protect your device and organization data."
- **OS Update Required:** "Your operating system is out of date; update required for security."
- **Risky App Detected:** "Uninstall flagged app to restore access."
- **Jailbroken Device:** "Device access blocked due to compromised security."
- **Unsafe Network:** "Disconnect from untrusted Wi-Fi."
- **Threat Detected (MTD):** "Resolve security threat to regain work app access."

Compliance Message Actions

The following list contains the actions that a user can perform:

- **Follow on-screen instructions:** These messages include clear steps to resolve issues (example, set a passcode, update OS, disconnect from risky Wi-Fi, and so on).
- **Act promptly:** Delays may result in temporary loss of access to work email, apps, or corporate data.
- **Use support resources:** If unsure, check the **Support** tab in Ivanti or contact your IT department.
- **Privacy assurance:** Compliance checks do not allow IT to view your personal data. The administrators can confirm that the security steps are complete and compliant

Importance of Compliance

The importance of compliance that an organization or user needs to abide are as follows:

- To protect the organization's data from breaches, ransomware, and cyberattacks.
- To ensure adherence to legal, regulatory, and internal security mandates.
- To maintain privacy by controlling only business-related activity, not personal content.
- To minimize threats that can impact both the organization and personal data on mixed-use devices.

Data Management

Containers and App Wrapping

Enterprise Data Containerization

Ivanti Go for iOS complies with global GDPR privacy regulations by using containers and app wrapping. Your personal information remains private and untracked. Ivanti Go for iOS only manages business-related information and managed apps. If you have any queries, use the app's **Support** tab or contact your administrator.

- **Secure Container:** Managed apps like business emails and documents are installed and run in an encrypted "container" area. Data in this container is protected and isolated from your personal apps and files.
- **App Wrapping:** Some apps are "wrapped" by Ivanti solutions. As a result, business policies such as password requirements and data restrictions apply only to business-related data, not to your personal apps or files.
- **Selective Wipe:** If your device is lost, stolen, or you leave the organization, only corporate data and apps in the container are wiped, and your personal data remains untouched.

Indication of Data Separation

- **Managed apps:** Managed work apps on iOS devices are indicated with a briefcase or business icon, as shown in the App Catalog section.
- **Personal apps remain private:** These are never listed or accessed by Ivanti solutions or admin consoles.
- **Device compliance:** Only business-related compliance metrics are tracked and displayed (example, whether encryption is enabled or the OS is updated).
- **Location services:** The user will retain the ability to enable or disable location services on their devices.

Device Status

The **Device Status** tab provides an overview of the device's security details and compliance state. You can learn and verify whether your device meets organizational security requirements. If your device is marked In Compliance, which means all necessary checks - such as operating system updates, security configurations, and threat scans that have passed successfully. This security check ensures that your device is secure and authorized to access organizational resources.

Features and Homescreen Guide

The following table details the most used features in Ivanti Go for iOS app:

Feature	Description
Home	Displays Device Compliance, alerts and notifications, security incidents, last update, and quick actions.
Apps@Work	Browse and install secure work apps from the app catalog; auto updates may be enforced.
Support	Displays the contact information, support site link, and additional information about the IT administrator.
Notifications	Alerts for compliance, updates, or security incidents.
Mobile Threat Defense (MTD)	Detects malware, risky networks, compromised devices.
Secure Tunnel or VPN	On-demand secure connection to organization resources and internal sites.
Settings	View compliance status, check security settings, and manage app permissions.
Log Collection & Diagnostics	The IT administrators can access technical logs and diagnostic information for troubleshooting.
Re-enroll device	Provisions to wipe the devices automatically and assist in re-enrolling and re-provisioning devices by retaining device applications.

Ivanti Go for iOS documentation

The following is a complete list of documentation for this product. However, the list of documents updated for specific versions will vary, depending on release requirements. Therefore, you might encounter documents from previous releases that still apply to the current release.

- [Go for iOS Release Notes](#)

Summary of new features, support and compatibility, known and resolved issues, and limitations.

- [Go for iOS User Guide](#)

Ivanti Go is a mobile application designed to work with the Ivanti Neurons for MDM, which supports iOS and Android platforms. It helps organizations securely manage and enable mobile device access to company resources.

Ivanti Tunnel

Ivanti Tunnel provides secure, seamless connectivity between managed mobile devices and organization resources. It enables encrypted access to internal networks, enterprise applications, and approved cloud services without requiring manual user interaction.

Ivanti Tunnel is automatically configured and managed by IT administrators as part of the device enrollment and management process, ensuring consistent security enforcement and user transparency.

Ivanti Tunnel is a mobile application that establishes an encrypted work network connection for managed devices. It secures data in transit when users access corporate email, applications, files, and internal web resources—whether those resources are hosted on premises or in the cloud.

Tunnel operates silently in the background and applies protection only to managed work traffic, leaving personal applications and data untouched.

Key Administrative Benefits

- Secure access to enterprise resources from any location
- Automatic encryption of managed application traffic
- No user sign in or manual VPN interaction required
- Separation of corporate and personal data
- Centralized configuration and policy enforcement
- Reduced support overhead for remote connectivity issues

Deployment and Enablement

- Ivanti Tunnel cannot be enabled by end users.
- It is automatically deployed and configured by administrators when:
 - The device is enrolled in Ivanti MDM
 - Tunnel is enabled within the organization's configuration
- If Tunnel is not enabled for an organization or user group, the app or VPN profile will not be visible on the device.

The absence of Tunnel on a device does not indicate an issue if the organization has not licensed or configured Tunnel.

For more information, see [Ivanti Tunnel for iOS Guide](#).

Additional configurations using key-value-pairs

KVPs (Key-value Pairs) are simple app settings made of a key (the name of a setting) and a value (what you want that setting to be). On Ivanti Go for iOS clients (like the Ivanti Go app), your company can use KVPs to turn features on or off or fine-tune how the app behaves - without needing an app update. The app reads these settings on company-managed iPhones and iPads when it starts or checks in, and applies them right away, so changes roll out quickly and consistently to the right users.

Using KVPs in Ivanti Go App Configurations

You can configure Key-Value Pairs (KVPs) within the Ivanti Go app settings to customize application.

Procedure

1. Open the **Ivanti Go app** in your AppCatalog.
2. Select **Configurations**.
3. Click **Add** to create a new **Apple App Configuration**.
4. Add your KVPs manually:
 - In the **Key** column, enter the configuration key you want to customize.
 - In the **Value** column, enter the value you want enforced on devices.
5. (Optional) Upload an existing *.plist* file containing predefined KVPs you wish to apply.
6. **Save** the configuration.
7. The updated KVPs will be applied to devices during their next check-in.

KVPs for customizing policy violation messages

These KVPs enable administrators to customize the messages sent to end users when Policy Violations are detected.

These KVPs for customization describes the KVPs and violation types available to administrators to customize Ivanti Go for iOS app behavior. These KVPs define app behavior such as providing detailed notifications to device users and export contacts from Ivanti Go for iOS.

The violation types are not mutually exclusive. If there are a set of violations, then a list of messages will be shown in the Ivanti Go for iOS.

Key Value Pairs (KVP)	Default Messages
compliance.message.COM PROMISED	Your device has been compromised because it has been jailbroken. Please properly return your device to a non-jailbroken state or contact your administrator for help resolving this issue.
compliance.message.DATA _PROTECTION_DISABLED	Corporate access has been disabled for data protection. Please contact your administrator for help resolving this issue.
compliance.message.OUT_ OF_CONTACT	Your iOS device is out of contact. Please contact your administrator for help resolving this issue.
compliance.message.APPS	Your device is missing apps that are required and/or it has apps that aren't allowed. Please add/remove necessary apps or contact your administrator for help resolving this issue.
compliance.message.MDM _DISABLED	Your device is out of compliance because MDM capability has been deactivated. Please re-enroll your device, or contact your administrator for help resolving this issue.
compliance.message.ROA MING	
compliance.message.gene ric	Corporate access has been disabled for an unspecified reason. Please contact your administrator for help resolving this issue.
compliance.message.head er	Your device is out of compliance for the following reason(s): When the violation type is CUSTOM or CUSTOM_NOTIFY_ONLY, the system displays standalone messages without a header.
compliance.message.CUST OM	An action may be required on your device. Please contact your admin as needed.
compliance.message.CUST OM_NOTIFY_ONLY	Your device is out of compliance, and a notification has been sent. Please refer to the notifications tab or your email for details.

If the violation types list does not include any violation with a mapped message, but it includes at least one violation without a mapped message, then display the default message:

- Corporate access has been disabled for an unspecified reason. Please contact your administrator for help resolving this issue.

If the messages list contains at least one violation message, display the following header above the list:
Your device is out of compliance for the following reason(s):

If you do not want to change a default message, do not include a key-value pair (KVP) for it. Only define KVPs for the messages you intend to modify.

Apps@Work

Apps@Work is your organization's secure app store that provides easy access to all the work-related applications you need. Instead of browsing public app stores such as the Apple App Store, Apps@Work offers a curated catalog of apps that your IT team has approved for your role. Every app listed here has been reviewed for security, relevance, and usability, ensuring you can trust the tools you install.

When you open Apps@Work, you can explore the catalog like other app store. You can:

- Browse for work related apps.
- View descriptions and screenshots that explain about an app and its benefits.
- Check installation status while using Apps@Work clearly shows which apps are already installed on your device.

Some apps may be:

- Required for your job,
- Recommended to support productivity, or
- Optional tools you can choose to install as needed.

This helps you easily identify what's available and what may need to be updated.

Installing Apps

Installing apps through Apps@Work is quick and effortless.

Simply tap an app to begin installation—no additional configuration, setup steps, or technical knowledge are required.

In many cases:

- Apps install automatically, and
- Updates are applied without manual action, ensuring you always have the latest, secure versions.

This automatic maintenance keeps your device secure and minimizes interruptions to your workflow.

Privacy and Security

Apps@Work is designed with your privacy in mind. It manages only work-related apps and does not access your personal apps or personal data.

Your personal space on the device remains completely private.

This separation ensures:

- Your organization can safely deploy work tools.
- You retain full control over your personal applications and information.

Benefits of Apps@Work

Apps@Work provides a convenient, centralized place to discover and install all your work apps. It helps you:

- Save time by avoiding public app store searches.
- Reduce confusion with a curated, role specific app catalog.

- Stay secure with verified, IT approved apps.
- Remain productive with seamless updates.

The Apps@Work screen includes the following tabs at the top:

- **Featured:** Highlights recommended apps
- **All apps:** Displays the complete list of apps available to the user
- **Categories:** Groups apps by functional category

For more information, see [iOS Apps@Work](#).

Common Threat Scenarios Detected by MTD

The common threat scenarios that mobile Threat Defense (MTD) detects are as follows:

- **Malware and Risky Apps:** If the apps are downloaded from unofficial app stores, or those requesting excessive permissions, then they are flagged as risk. MTD alerts you and guides you to uninstall such apps.
- **OS Vulnerabilities:** If your operating system is outdated or known vulnerable, you will receive a compliance alert directing you to update your device software.
- **Jailbroken or Rooted Device:** If your device is modified, reducing security, MTD blocks access to organization data until restored.
- **Unsafe Wi-Fi Networks:** If you connect to public or untrusted networks, MTD enables for threats such as "man-in-the-middle" attacks. MTD prompts you to disconnect or switch networks.
- **Phishing & Network Attacks:** If there are some advanced MTD features, they can detect attempts to steal credentials or intercept communications on untrusted networks.
- **Configuration Issues:** If the weak security settings, such as disabled encryption or weak passwords, are present, then the issue is flagged.

Compliance Messages

Compliance messages in Ivanti Go for iOS appear because your organization enforces specific security rules and standards to protect sensitive business data. These policies apply to both corporate-owned and personal - Bring Your Own Device (BYOD) devices to ensure they remain secure, trustworthy, and eligible for accessing organizations resources and apps. You need to fulfill these compliance requirements to help safeguard business information and maintain a secure work environment.

Managing Rule Ownership and Responsibilities

Your organization's IT Administrator defines security policies in the Ivanti platform. These policies determine the following requirements that the devices must meet:

- Mandatory pass codes and screen locks
- Device encryption
- Latest OS or software updates
- Secure Wi-Fi usage
- No risky apps or configurations (examples: Malware, Jailbreaking)
- Mobile Threat Defense (MTD) actions
- Every organization's standards may differ based on industry regulations, security needs, and risk profiles.

Common Compliance Messages

The following list contains compliance messages that will appear on the devices:

- **Passcode Required:** "Please set a device passcode to access organization resources."
- **Encryption Needed:** "Enable encryption to protect your device and organization data."
- **OS Update Required:** "Your operating system is out of date; update required for security."
- **Risky App Detected:** "Uninstall flagged app to restore access."
- **Jailbroken Device:** "Device access blocked due to compromised security."
- **Unsafe Network:** "Disconnect from untrusted Wi-Fi."
- **Threat Detected (MTD):** "Resolve security threat to regain work app access."

Compliance Message Actions

The following list contains the actions that a user can perform:

- **Follow on-screen instructions:** These messages include clear steps to resolve issues (example, set a passcode, update OS, disconnect from risky Wi-Fi, and so on).
- **Act promptly:** Delays may result in temporary loss of access to work email, apps, or corporate data.
- **Use support resources:** If unsure, check the **Support** tab in Ivanti or contact your IT department.
- **Privacy assurance:** Compliance checks do not allow IT to view your personal data. The administrators can confirm that the security steps are complete and compliant

Importance of Compliance

The importance of compliance that an organization or user needs to abide are as follows:

- To protect the organization's data from breaches, ransomware, and cyberattacks.
- To ensure adherence to legal, regulatory, and internal security mandates.
- To maintain privacy by controlling only business-related activity, not personal content.
- To minimize threats that can impact both the organization and personal data on mixed-use devices.

Data Management

Containers and App Wrapping

Enterprise Data Containerization

Ivanti Go for iOS complies with global GDPR privacy regulations by using containers and app wrapping. Your personal information remains private and untracked. Ivanti Go for iOS only manages business-related information and managed apps. If you have any queries, use the app's **Support** tab or contact your administrator.

- **Secure Container:** Managed apps like business emails and documents are installed and run in an encrypted "container" area. Data in this container is protected and isolated from your personal apps and files.
- **App Wrapping:** Some apps are "wrapped" by Ivanti solutions. As a result, business policies such as password requirements and data restrictions apply only to business-related data, not to your personal apps or files.
- **Selective Wipe:** If your device is lost, stolen, or you leave the organization, only corporate data and apps in the container are wiped, and your personal data remains untouched.

Indication of Data Separation

- **Managed apps:** Managed work apps on iOS devices are indicated with a briefcase or business icon, as shown in the App Catalog section.
- **Personal apps remain private:** These are never listed or accessed by Ivanti solutions or admin consoles.
- **Device compliance:** Only business-related compliance metrics are tracked and displayed (example, whether encryption is enabled or the OS is updated).
- **Location services:** The user will retain the ability to enable or disable location services on their devices.

Device Status

The **Device Status** tab provides an overview of the device's security details and compliance state. You can learn and verify whether your device meets organizational security requirements. If your device is marked In Compliance, which means all necessary checks - such as operating system updates, security configurations, and threat scans that have passed successfully. This security check ensures that your device is secure and authorized to access organizational resources.

Features and Homescreen Guide

The following table details the most used features in Ivanti Go for iOS app:

Feature	Description
Home	Displays Device Compliance, alerts and notifications, security incidents, last update, and quick actions.
Apps@Work	Browse and install secure work apps from the app catalog; auto updates may be enforced.
Support	Displays the contact information, support site link, and additional information about the IT administrator.
Notifications	Alerts for compliance, updates, or security incidents.
Mobile Threat Defense (MTD)	Detects malware, risky networks, compromised devices.
Secure Tunnel or VPN	On-demand secure connection to organization resources and internal sites.
Settings	View compliance status, check security settings, and manage app permissions.
Log Collection & Diagnostics	The IT administrators can access technical logs and diagnostic information for troubleshooting.
Re-enroll device	Provisions to wipe the devices automatically and assist in re-enrolling and re-provisioning devices by retaining device applications.

Ivanti Tunnel

Ivanti Tunnel provides secure, seamless connectivity between managed mobile devices and organization resources. It enables encrypted access to internal networks, enterprise applications, and approved cloud services without requiring manual user interaction.

Ivanti Tunnel is automatically configured and managed by IT administrators as part of the device enrollment and management process, ensuring consistent security enforcement and user transparency.

Ivanti Tunnel is a mobile application that establishes an encrypted work network connection for managed devices. It secures data in transit when users access corporate email, applications, files, and internal web resources—whether those resources are hosted on premises or in the cloud.

Tunnel operates silently in the background and applies protection only to managed work traffic, leaving personal applications and data untouched.

Key Administrative Benefits

- Secure access to enterprise resources from any location
- Automatic encryption of managed application traffic
- No user sign in or manual VPN interaction required
- Separation of corporate and personal data
- Centralized configuration and policy enforcement
- Reduced support overhead for remote connectivity issues

Deployment and Enablement

- Ivanti Tunnel cannot be enabled by end users.
- It is automatically deployed and configured by administrators when:
 - The device is enrolled in Ivanti MDM
 - Tunnel is enabled within the organization's configuration
- If Tunnel is not enabled for an organization or user group, the app or VPN profile will not be visible on the device.

The absence of Tunnel on a device does not indicate an issue if the organization has not licensed or configured Tunnel.

For more information, see [Ivanti Tunnel for iOS Guide](#).

Notifications

Tap the **Notifications** icon (bell icon) to view important alerts about your device's security and compliance status.

- If you see a green checkmark, your device is fully compliant, and no action is needed.
- If you see a badge count, tap the icon to review and resolve pending notifications such as OS updates, risky apps, or network issues.

Privacy and Data Separation

Ivanti Go for iOS complies with Privacy and Data Separation, and an organization cannot access your personal messages, photos, contacts, or apps. Only work-related apps and data managed by your organization are protected.

- **Personal Data:** Your organization cannot view or share your personal files, photos, conversations, or private apps.
- **Corporate Data:** An organization can encrypt and protect corporate data if necessary. It can remotely wipe only the business-related content, if needed.
- **GDPR and Data Privacy:** All apps should comply with privacy laws such as the General Data Protection Regulation (GDPR), ensuring business-related and personal data are separated, and organizational policies are enforced without intruding on personal data.

Privacy, GDPR, and Data Protection in Ivanti Go for iOS

Privacy Protection

Ivanti Go for iOS ensures that your personal information (PII) remains private, secure, and under your control, even when your device is managed for business use. The apps strictly limit what data your organization can view or control, focusing only on business-related content.

- **PII data:** Data such as contacts, photos, text messages, browsing history, personal apps, and location is never shared with IT or administrators.
- **Corporate data:** Managed apps, documents, business emails, and corporate settings are subject to security policies (encryption, remote wipe, and compliance enforcement).

GDPR and Data Privacy

Ivanti Go for iOS complies with privacy laws like General Data Protection Regulation (GDPR) to ensure the following:

- **Data Separation:** Maintains a separation between business-related and personal data.
- **Data Minimization:** Essential business Metadata (device type, OS version, and compliance status) is visible to the administrators.
- **Explicit Transparency:** Clear communication about which data is monitored.
- **Encrypted Data:** All business-related data and communications are encrypted.
- **Consent and Controls:** Users can review the collected data, withdraw consent, or request deletion of data in accordance with the organization's legal policies.
- **Breach Notification:** Enforcement of strict notifications and resolution steps, if managed data is involved in a breach.

Privacy Settings

An organization should value the user's privacy while ensuring secure access to business resources. Ivanti Go for iOS does not sell or share any data with third parties for any reason.

The **Privacy** settings detail how Ivanti Go for iOS handles your data and what your organization can access.

- **Personal content remains private:** Your organization cannot use Ivanti Go for iOS to access personal content on your devices.
- **What's accessible by my organization?:** Some device details are required to provide secure mobility services.
- **What actions can my organization take?:** If your device is lost or stolen, your organization can take security measures to protect your data.

Personal Content Privacy:

The following personal information is never accessible by an organization:

- **Personal Email:** An organization cannot view the details of your personal email accounts.
- **Text Messages:** iMessage or SMS content remains private.
- **Personal Contacts:** Only contacts associated with your work account are visible.
- **Photos and Videos:** Media stored on your device is not accessible.
- **Voicemail:** An organization cannot monitor voice mail communication.

Accessible Information:

The following information is accessible by an organization for security reasons:

- **Device Details:** Model name, OS version, and roaming status of the devices.
- **Device Location:** Last known location to help recover lost or stolen devices.
- **Installed Apps:** Names and versions of apps from the organization's app catalog (app content is not collected).

Action on Lost or Stolen Devices:

If your device is lost or stolen, you and your organization can perform the following actions:

- **Clear Device Passcode:** Reset the passcode remotely if you have forgotten it.
- **Lock Device:** You can lock the device remotely and display contact information for recovery.
- **Erase Device:** Wipe the device remotely to protect sensitive data.

Self-Service Return to Service

You can select **Return to Service** to automatically re-enroll the device after the data is erased. This eliminates the need to manually re-enroll the device after a wipe. Applicable only to iOS 18 or later devices enrolled in DEP mode.

If you want the **Return to Service** option to be visible to end users, you must set a new Key-Value Pair (KVP) setting in the managed app configurations.

Return to Service is a secure and automated work flow that:

- Wipes all user data from the device
- Re-provisions the device with corporate management settings
- Automatically re-enrolls device for new users

This process ensures organizational compliance and protects user privacy. For more information, see *iOS Go Advanced Features* in *Ivanti Neurons for MDM Administrator Guide*.

Use Case: Shared and Hospital Devices

In environments such as hospitals, retail stores, clinics, or other shared device scenarios, administrators can enable Return to Service within the Ivanti app.

This allows employees (such as nurses, clinicians, or shift workers) to initiate a secure device reset themselves, which eliminates the need to submit an IT support request.

Example: When a patient is discharged or moved to another room, staff can immediately reset the device and prepare it for the next patients securely and within minutes.

Procedure

Once enabled by an administrator, the workflow is as follows:

1. Log into the **Ivanti Go app** on the device.
2. Select **Return to Service** from the app menu or settings.

Administrator must enable **Return to Service** option to be visible to end users

1. The device performs a secure wipe, removing:
 - All user data
 - Applications
 - Settings
2. After the wipe, the device:
 - Automatically re-enrolls into MDM
 - Reapplies to organization policies and applications
 - Re-installs required organizations apps
3. The device is immediately ready to be handed to:

- Another employee
- A new patient
- The next shift user

Security Features

- **Device Encryption:** Ensures all business-related sensitive data is stored in an encrypted form on your device.
- **Remote Wipe:** If the device is lost, stolen, or you leave the organization, only business-related data and apps are wiped away, not your personal files.
- **Secure App Container:** Some apps and data are kept inside a protected workspace, further separating work and personal apps.
- **Jailbreak or Root Detection:** If your device is compromised (jailbroken), the app may block access to organization data until it is rectified.
- **Password Policies:** If required, you will need a passcode or biometric security.
- **Network Protection:** Organization data is kept safe while connected to public Wi-Fi using secure VPN tunnels.
- **Mobile Threat Defense:** Notifies you of threats and provides one-click fixes or guides you to contact the IT administrator.

Frequently Used Tabs

- **App Catalog:** Choose to install or open managed apps. Some apps may update automatically.
- **Support:** Read how-to guides, get help fixing issues, or contact IT directly.
- **Notifications:** Review and act on compliance alerts, update requests, and security messages promptly.
- **Settings:** View device status, fix compliance issues (for example, enabling a passcode), view your privacy rights, security features, and access and send logs on request.

Troubleshooting Tips

- **Compliance Problems:** The Ivanti Go for iOS app displays no passcode, outdated software, and so on. Follow the in-app instructions to resolve the issue.
- **Cannot Install Apps:** Make sure device meets security requirements such as passcode and latest OS.
- **VPN or Tunnel Issue:** If you cannot access VPN or Tunnel, check your network connection and speed, try toggling airplane mode, or restart your device. If issues persist, contact the IT administrator.
- **Threat Detected:** Ivanti Go for iOS app provides information and steps to remove risky apps or recommends updating the device OS to the latest version.
- **Lost Access (Quarantined):** Use **Return to Service**, the Ivanti Go for iOS app guides you through recovery. For unresolved problems, contact IT administrators using the Support tab.
- **Log Collection:** The IT administrators can request Logs and Diagnostics for troubleshooting. Access the log collection feature from the Settings tab and share the logs or diagnostic information.

Settings

The **Settings** section allows you to manage troubleshooting, security, and general app preferences. It includes the following categories:

- Help & Feedback
- Security
- General

Help & Feedback

Using **Help & Feedback**, you can access tools to resolve generic issues and gather diagnostic information.

Troubleshoot Menu

The **Troubleshoot** option provides the following options:

- **Check for Updates:** Ensures your app is running the latest version.
- **Re-enroll Device:** Re-register your devices with the management system if an enrollment issue occurs.
- **Send Ivanti Go for iOS Logs:** Collect and share logs for support. When selected, a ZIP file is generated, which can be shared using email, messages, or saved to files.
- **Enhanced Logging:** Toggle advanced logging for detailed troubleshooting.

Security

The Security section in Ivanti Go for iOS provides quick access to essential features like Ivanti Tunnel for secure connectivity and Manage Devices for overseeing enrolled devices.

Tunnel

Ivanti Tunnel provides secure access to enterprise data including the following options:

- **VPN:** Toggle to disable or enable VPN access.
- **Enable Logging:** Toggle to enable or disable logs.
- **Log Level:** Set various log levels like Error, Warning, Info, Debug, Session, and Packet, with the option to clear all logs.
- **Email Debug Info:** Share the debug information through email.
- **Share Debug Info:** Share or save debug information in various formats.
- **Clear Cache:** Removes locally cached data from the Ivanti Tunnel app.
- **License Information:** Displays the license information.

Manage Devices

Manage Devices allows you to view and control the status of your enrolled devices, including checking compliance and performing basic actions like updating or re-enrolling a device.

Additionally, you must provide your organization with credentials during the authentication process. You can perform the following actions:

- Navigate to **Settings > My Devices** to access the feature.
- Manage your current device and other enrolled devices.
- Authentication is required to view device details:
 - Tap **Show my devices**.
 - Enter your organization username and password when prompted.

Manage Devices provides a convenient way to manage multiple devices without leaving the Ivanti Go app.

Ensures secure access through organization credentials.

General

The **General** section provides you with information about the application and access to privacy related details.

About

The **About** screen displays app version and licensing details. The **About** screen provides key information about the **Ivanti Go for iOS** application. You can access this screen by navigating to **Settings > About**.

- **Product Details:**
 - **Version:** Displays the current version of the app, including build details.
 - **Built:** Displays the release date and time when the build.
 - **More Info:** Provides a link to Ivanti's product page for additional details.
- **Licenses:** Provides all license details such as version number, copyright and license information, license agreements, links to the End User License Agreement, links to third-party software declarations, and more.
- **EULA:** The End User License and Services Agreement (EULA) outlines the terms and conditions for using Ivanti software or SaaS offerings. You should review these terms before installing or using the application.

Support Tab

The **Support** tab in the Ivanti Go for iOS app, enables administrators to display contact details and useful links to end-users. This tab can be customized and set as the home screen with the following fields:

- Contact Name
- Support Email Address
- Support Phone Number
- Website URL or Useful Links
- Additional Information

Admins can now configure these fields using the server, with field validation enforced for accuracy.

Clients display the configured tab and links on their app, enabling them to conveniently contact support or visit the [support site](#) for assistance.

Accessing the Support Tab

Procedure

1. Open **Ivanti Go** on your device.
2. Look for the **Support** icon (usually found at the bottom or main menu of the app).
3. Select the **Support** to access all support information.

MTD functionality

Mobile Threat Defense (MTD) is a security solution designed to protect mobile devices from cyber threats without compromising user privacy.

- **Real-time Threat Detection:** Monitors device apps, operating system integrity, and network connections for vulnerabilities or suspicious activity.
- **Automatic Alerts:** Notifies you instantly if suspicious activity, risky apps, unsafe networks, or device vulnerabilities are detected.
- **Guided Remediation:** Provides step-by-step instructions to resolve issues quickly (example, uninstalling an unsafe app).
- **No Intrusion on Privacy:** Does not access personal content like messages, browsing history, or files, but only checks for security risks.
- **Seamless User Experience:** Most scans run silently in the background; you're only prompted when action is required.

Mobile Threat Defense (MTD)

MTD is a built-in security feature available in Ivanti Go app. MTD continuously monitors your device for cyber threats that could affect both work and personal use. MTD monitors risks and vulnerabilities, then guides you to take correct actions - keeping your device, your data, and organizations resources secure.

Mobile Threat Defense (MTD) protects managed devices from mobile threats and vulnerabilities affecting devices, networks, and applications. For information on MTD-related features, as applicable for the current release, see the *Mobile Threat Defense Solution Guide* for your platform, available under the MOBILE THREAT DEFENSE section on the [Ivanti Product Documentation page](#).

Each version of the MTD guide contains all Mobile Threat Defense features that are currently fully tested and available for use on both server and client environments. Because of the gap between server and client releases, new versions of the MTD guide are made available with the final release in the series when the features are fully functional.

Actions after Detecting a Compliance Violation

Ivanti Go for iOS will immediately notify you about the threat by displaying a warning with clear information about the issue.

You need to perform the following actions after it detects a threat:

- **Remove risky apps:** Uninstall the applications that were flagged by Ivanti MTD.
- **Update your device's OS:** Follow the device prompts to install security updates.
- **Change Wi-Fi network:** Disconnect from unsafe networks and reconnect using secure Wi-Fi or mobile data.
- **Restore security settings:** Immediately enable encryption, set a strong passcode, or re-enable security features as required.
- **Temporary Access Block:** For serious issues (for example, if your device's security is compromised), your organizations data and apps may be temporarily inaccessible until the threat is resolved.
- **Help Resources:** Use the **Support** tab to request IT assistance if you are unsure how to fix the issues.

Notifications

Tap the **Notifications** icon (bell icon) to view important alerts about your device's security and compliance status.

- If you see a green checkmark, your device is fully compliant, and no action is needed.
- If you see a badge count, tap the icon to review and resolve pending notifications such as OS updates, risky apps, or network issues.

Privacy and Data Separation

Ivanti Go for iOS complies with Privacy and Data Separation, and an organization cannot access your personal messages, photos, contacts, or apps. Only work-related apps and data managed by your organization are protected.

- **Personal Data:** Your organization cannot view or share your personal files, photos, conversations, or private apps.
- **Corporate Data:** An organization can encrypt and protect corporate data if necessary. It can remotely wipe only the business-related content, if needed.
- **GDPR and Data Privacy:** All apps should comply with privacy laws such as the General Data Protection Regulation (GDPR), ensuring business-related and personal data are separated, and organizational policies are enforced without intruding on personal data.

Privacy, GDPR, and Data Protection in Ivanti Go for iOS

Privacy Protection

Ivanti Go for iOS ensures that your personal information (PII) remains private, secure, and under your control, even when your device is managed for business use. The apps strictly limit what data your organization can view or control, focusing only on business-related content.

- **PII data:** Data such as contacts, photos, text messages, browsing history, personal apps, and location is never shared with IT or administrators.
- **Corporate data:** Managed apps, documents, business emails, and corporate settings are subject to security policies (encryption, remote wipe, and compliance enforcement).

GDPR and Data Privacy

Ivanti Go for iOS complies with privacy laws like General Data Protection Regulation (GDPR) to ensure the following:

- **Data Separation:** Maintains a separation between business-related and personal data.
- **Data Minimization:** Essential business Metadata (device type, OS version, and compliance status) is visible to the administrators.
- **Explicit Transparency:** Clear communication about which data is monitored.
- **Encrypted Data:** All business-related data and communications are encrypted.
- **Consent and Controls:** Users can review the collected data, withdraw consent, or request deletion of data in accordance with the organization's legal policies.
- **Breach Notification:** Enforcement of strict notifications and resolution steps, if managed data is involved in a breach.

Privacy Settings

An organization should value the user's privacy while ensuring secure access to business resources. Ivanti Go for iOS does not sell or share any data with third parties for any reason.

The **Privacy** settings detail how Ivanti Go for iOS handles your data and what your organization can access.

- **Personal content remains private:** Your organization cannot use Ivanti Go for iOS to access personal content on your devices.
- **What's accessible by my organization?:** Some device details are required to provide secure mobility services.
- **What actions can my organization take?:** If your device is lost or stolen, your organization can take security measures to protect your data.

Personal Content Privacy:

The following personal information is never accessible by an organization:

- **Personal Email:** An organization cannot view the details of your personal email accounts.
- **Text Messages:** iMessage or SMS content remains private.
- **Personal Contacts:** Only contacts associated with your work account are visible.
- **Photos and Videos:** Media stored on your device is not accessible.
- **Voicemail:** An organization cannot monitor voice mail communication.

Accessible Information:

The following information is accessible by an organization for security reasons:

- **Device Details:** Model name, OS version, and roaming status of the devices.
- **Device Location:** Last known location to help recover lost or stolen devices.
- **Installed Apps:** Names and versions of apps from the organization's app catalog (app content is not collected).

Action on Lost or Stolen Devices:

If your device is lost or stolen, you and your organization can perform the following actions:

- **Clear Device Passcode:** Reset the passcode remotely if you have forgotten it.
- **Lock Device:** You can lock the device remotely and display contact information for recovery.
- **Erase Device:** Wipe the device remotely to protect sensitive data.

Self-Service Return to Service

You can select **Return to Service** to automatically re-enroll the device after the data is erased. This eliminates the need to manually re-enroll the device after a wipe. Applicable only to iOS 18 or later devices enrolled in DEP mode.

If you want the **Return to Service** option to be visible to end users, you must set a new Key-Value Pair (KVP) setting in the managed app configurations.

Return to Service is a secure and automated work flow that:

- Wipes all user data from the device
- Re-provisions the device with corporate management settings
- Automatically re-enrolls device for new users

This process ensures organizational compliance and protects user privacy. For more information, see *iOS Go Advanced Features* in *Ivanti Neurons for MDM Administrator Guide*.

Use Case: Shared and Hospital Devices

In environments such as hospitals, retail stores, clinics, or other shared device scenarios, administrators can enable Return to Service within the Ivanti app.

This allows employees (such as nurses, clinicians, or shift workers) to initiate a secure device reset themselves, which eliminates the need to submit an IT support request.

Example: When a patient is discharged or moved to another room, staff can immediately reset the device and prepare it for the next patients securely and within minutes.

Procedure

Once enabled by an administrator, the workflow is as follows:

1. Log into the **Ivanti Go app** on the device.
2. Select **Return to Service** from the app menu or settings.

Administrator must enable **Return to Service** option to be visible to end users

1. The device performs a secure wipe, removing:
 - All user data
 - Applications
 - Settings
2. After the wipe, the device:
 - Automatically re-enrolls into MDM
 - Reapplies to organization policies and applications
 - Re-installs required organizations apps
3. The device is immediately ready to be handed to:

- Another employee
- A new patient
- The next shift user

Security Features

- **Device Encryption:** Ensures all business-related sensitive data is stored in an encrypted form on your device.
- **Remote Wipe:** If the device is lost, stolen, or you leave the organization, only business-related data and apps are wiped away, not your personal files.
- **Secure App Container:** Some apps and data are kept inside a protected workspace, further separating work and personal apps.
- **Jailbreak or Root Detection:** If your device is compromised (jailbroken), the app may block access to organization data until it is rectified.
- **Password Policies:** If required, you will need a passcode or biometric security.
- **Network Protection:** Organization data is kept safe while connected to public Wi-Fi using secure VPN tunnels.
- **Mobile Threat Defense:** Notifies you of threats and provides one-click fixes or guides you to contact the IT administrator.

Frequently Used Tabs

- **App Catalog:** Choose to install or open managed apps. Some apps may update automatically.
- **Support:** Read how-to guides, get help fixing issues, or contact IT directly.
- **Notifications:** Review and act on compliance alerts, update requests, and security messages promptly.
- **Settings:** View device status, fix compliance issues (for example, enabling a passcode), view your privacy rights, security features, and access and send logs on request.

Troubleshooting Tips

- **Compliance Problems:** The Ivanti Go for iOS app displays no passcode, outdated software, and so on. Follow the in-app instructions to resolve the issue.
- **Cannot Install Apps:** Make sure device meets security requirements such as passcode and latest OS.
- **VPN or Tunnel Issue:** If you cannot access VPN or Tunnel, check your network connection and speed, try toggling airplane mode, or restart your device. If issues persist, contact the IT administrator.
- **Threat Detected:** Ivanti Go for iOS app provides information and steps to remove risky apps or recommends updating the device OS to the latest version.
- **Lost Access (Quarantined):** Use **Return to Service**, the Ivanti Go for iOS app guides you through recovery. For unresolved problems, contact IT administrators using the Support tab.
- **Log Collection:** The IT administrators can request Logs and Diagnostics for troubleshooting. Access the log collection feature from the Settings tab and share the logs or diagnostic information.

Settings

The **Settings** section allows you to manage troubleshooting, security, and general app preferences. It includes the following categories:

- Help & Feedback
- Security
- General

Help & Feedback

Using **Help & Feedback**, you can access tools to resolve generic issues and gather diagnostic information.

Troubleshoot Menu

The **Troubleshoot** option provides the following options:

- **Check for Updates:** Ensures your app is running the latest version.
- **Re-enroll Device:** Re-register your devices with the management system if an enrollment issue occurs.
- **Send Ivanti Go for iOS Logs:** Collect and share logs for support. When selected, a ZIP file is generated, which can be shared using email, messages, or saved to files.
- **Enhanced Logging:** Toggle advanced logging for detailed troubleshooting.

Security

The Security section in Ivanti Go for iOS provides quick access to essential features like Ivanti Tunnel for secure connectivity and Manage Devices for overseeing enrolled devices.

Tunnel

Ivanti Tunnel provides secure access to enterprise data including the following options:

- **VPN:** Toggle to disable or enable VPN access.
- **Enable Logging:** Toggle to enable or disable logs.
- **Log Level:** Set various log levels like Error, Warning, Info, Debug, Session, and Packet, with the option to clear all logs.
- **Email Debug Info:** Share the debug information through email.
- **Share Debug Info:** Share or save debug information in various formats.
- **Clear Cache:** Removes locally cached data from the Ivanti Tunnel app.
- **License Information:** Displays the license information.

Manage Devices

Manage Devices allows you to view and control the status of your enrolled devices, including checking compliance and performing basic actions like updating or re-enrolling a device.

Additionally, you must provide your organization with credentials during the authentication process. You can perform the following actions:

- Navigate to **Settings > My Devices** to access the feature.
- Manage your current device and other enrolled devices.
- Authentication is required to view device details:
 - Tap **Show my devices**.
 - Enter your organization username and password when prompted.

Manage Devices provides a convenient way to manage multiple devices without leaving the Ivanti Go app.

Ensures secure access through organization credentials.

General

The **General** section provides you with information about the application and access to privacy related details.

About

The **About** screen displays app version and licensing details. The **About** screen provides key information about the **Ivanti Go for iOS** application. You can access this screen by navigating to **Settings > About**.

- **Product Details:**
 - **Version:** Displays the current version of the app, including build details.
 - **Built:** Displays the release date and time when the build.
 - **More Info:** Provides a link to Ivanti's product page for additional details.
- **Licenses:** Provides all license details such as version number, copyright and license information, license agreements, links to the End User License Agreement, links to third-party software declarations, and more.
- **EULA:** The End User License and Services Agreement (EULA) outlines the terms and conditions for using Ivanti software or SaaS offerings. You should review these terms before installing or using the application.

Support Tab

The **Support** tab in the Ivanti Go for iOS app, enables administrators to display contact details and useful links to end-users. This tab can be customized and set as the home screen with the following fields:

- Contact Name
- Support Email Address
- Support Phone Number
- Website URL or Useful Links
- Additional Information

Admins can now configure these fields using the server, with field validation enforced for accuracy.

Clients display the configured tab and links on their app, enabling them to conveniently contact support or visit the [support site](#) for assistance.

Accessing the Support Tab

Procedure

1. Open **Ivanti Go** on your device.
2. Look for the **Support** icon (usually found at the bottom or main menu of the app).
3. Select the **Support** to access all support information.

MTD functionality

Mobile Threat Defense (MTD) is a security solution designed to protect mobile devices from cyber threats without compromising user privacy.

- **Real-time Threat Detection:** Monitors device apps, operating system integrity, and network connections for vulnerabilities or suspicious activity.
- **Automatic Alerts:** Notifies you instantly if suspicious activity, risky apps, unsafe networks, or device vulnerabilities are detected.
- **Guided Remediation:** Provides step-by-step instructions to resolve issues quickly (example, uninstalling an unsafe app).
- **No Intrusion on Privacy:** Does not access personal content like messages, browsing history, or files, but only checks for security risks.
- **Seamless User Experience:** Most scans run silently in the background; you're only prompted when action is required.

Mobile Threat Defense (MTD)

MTD is a built-in security feature available in Ivanti Go app. MTD continuously monitors your device for cyber threats that could affect both work and personal use. MTD monitors risks and vulnerabilities, then guides you to take correct actions - keeping your device, your data, and organizations resources secure.

Mobile Threat Defense (MTD) protects managed devices from mobile threats and vulnerabilities affecting devices, networks, and applications. For information on MTD-related features, as applicable for the current release, see the *Mobile Threat Defense Solution Guide* for your platform, available under the MOBILE THREAT DEFENSE section on the [Ivanti Product Documentation page](#).

Each version of the MTD guide contains all Mobile Threat Defense features that are currently fully tested and available for use on both server and client environments. Because of the gap between server and client releases, new versions of the MTD guide are made available with the final release in the series when the features are fully functional.

Actions after Detecting a Compliance Violation

Ivanti Go for iOS will immediately notify you about the threat by displaying a warning with clear information about the issue.

You need to perform the following actions after it detects a threat:

- **Remove risky apps:** Uninstall the applications that were flagged by Ivanti MTD.
- **Update your device's OS:** Follow the device prompts to install security updates.
- **Change Wi-Fi network:** Disconnect from unsafe networks and reconnect using secure Wi-Fi or mobile data.
- **Restore security settings:** Immediately enable encryption, set a strong passcode, or re-enable security features as required.
- **Temporary Access Block:** For serious issues (for example, if your device's security is compromised), your organizations data and apps may be temporarily inaccessible until the threat is resolved.
- **Help Resources:** Use the **Support** tab to request IT assistance if you are unsure how to fix the issues.