# *2023 Release Notes*

IBM

# Contents

# Release Notes

MaaS360 product release notes for 2023

## MaaS360 Cloud Features

| Release Version | Release Date | Release Details |
|---|---|---|
| 10.90x | See Release Summary | "What's New Since 10.90 Release Notes" on page 6 |
| 10.90 | 19 August 2023 | "Release Notes for 10.90" on page 8 |
| 10.89x | See Release Summary | "What's New Since 10.89 Release Notes" on page 11 |
| 10.89 | 17 March 2023 | "Release Notes for 10.89" on page 15 |
| 10.88x | See Release Summary | "What's New Since 10.88 Release Notes" on page 17 |
| 10.88 | 02 December 2022 | Release notes for 10.88 |

## MaaS360 Cloud Fixes

| Fix Version | Fix Date | Fix Details |
|---|---|---|
| December 2023 Daily Fixes | Month of December | "December 2023 Daily Fixes Summary" on page 18 |
| November 2023 Daily Fixes | Month of November | "November 2023 Daily Fixes Summary" on page 18 |
| October 2023 Daily Fixes | Month of October | "October 2023 Daily Fixes Summary" on page 18 |
| September 2023 Daily Fixes | Month of September | "September 2023 Daily Fixes Summary" on page 19 |
| August 2023 Daily Fixes | Month of August | "August 2023 Daily Fixes Summary" on page 20 |
| July 2023 Daily Fixes | Month of July | "July 2023 Daily Fixes Summary" on page 21 |
| June 2023 Daily Fixes | Month of June | "June 2023 Daily Fixes Summary" on page 22 |
| May 2023 Daily Fixes | Month of May | "May 2023 Daily Fixes Summary" on page 23 |
| April 2023 Daily Fixes | Month of April | "April 2023 Daily Fixes Summary" on page 24 |
| March 2023 Daily Fixes | Month of March | "March 2023 Daily Fixes Summary" on page 26 |
| 10.89 Release Fixes | 10.89 | "10.89 Release Fix Summary" on page 26 |

| Fix Version | Fix Date | Fix Details |
|---|---|---|
| February 2023 Daily Fixes | Month of February | "February 2023 Daily Fixes Summary" on page 27 |
| January 2023 Daily Fixes | Month of January | "January 2023 Daily Fixes Summary" on page 28 |

## MaaS360 Cloud Extender and Mobile Enterprise Gateway

### Current Version of Cloud Extender Core Agent: v3.000.001.109

For instructions on subscribing to release candidate of Cloud Extender modules, see https://www.ibm.com/support/pages/node/1078587

| Release Version | Modules in Version | Release Candidate Elevation Date | Distribution Date(s) | Release Details |
|---|---|---|---|---|
| 3.000.400 Modules and Agent | MaaS360 VPN<br>Mobile Enterprise Gateway<br>Java SDK | 7 December 2023 | | "Cloud Extender 3.000.400 Release Notes" on page 28 |
| 3.000.300 Modules and Agent | MaaS360 VPN<br>Certification Integration | 14 November 2023 | | "Cloud Extender 3.000.300 Release Notes" on page 29 |
| 3.000.250 Modules and Agent | Cloud Extender Base<br>MaaS360 Configuration Utility<br>User Authentication<br>MaaS360 VPN<br>PKI Certificates<br>Core Installer | 2 October 2023 | | "Cloud Extender 3.000.250 Release Notes" on page 29 |
| 3.000.200/210 Modules and Agent | MaaS360 VPN<br>Mobile Enterprise Gateway | 31 August 2023 | | "Cloud Extender 3.000.200/210 Release Notes" on page 31 |
| 3.00.100 Modules and Agent | Cloud Extender Base<br>MaaS360 Configuration Utility<br>Exchange ActiveSync<br>User Authentication | 15 May 2023 | June 2023 | "Cloud Extender 3.000.100 Release Notes" on page 31 |

| Release Version | Modules in Version | Release Candidate Elevation Date | Distribution Date(s) | Release Details |
|---|---|---|---|---|
| | MaaS360 VPN<br>Mobile Enterprise Gateway<br>PKI Certificates<br>Core Installer | | | |
| 3.00.001 Modules and Agent | Cloud Extender Base<br>MaaS360 Configuration Utility<br>Email Notification module<br>User Visibility LDAP<br>Core Installer | 06 December 2022 | 07 December - 20 December 2022 | "Cloud Extender 3.00.001 Release Notes" on page 33 |

## MaaS360 for Android

| Release Version | Release Date | Release Details | Apps Released with this Version |
|---|---|---|---|
| 8.41/8.40 | 04 January 2023 | Android 8.41/8.40 Release Notes | MaaS360 MDM for Android |
| 8.35 | 18 October 2023 | Android 8.35 Release Notes | MaaS360 MDM for Android, MaaS360 Docs |
| 8.30 | 24 August 2023 | "Android 8.30 Release Notes" on page 35 | Core App, Secure Mail, Secure Browser, Secure Editor, Secure Viewer, Remote Support, VPN, Kiosk |
| 8.26 | 15 June 2023 | Android 8.26 Release Notes | Core app |
| 8.25 | 02 June 2023 | "Android 8.25 Release Notes" on page 36 | Core App, Secure Mail, Secure Browser, Secure Editor, Secure Viewer, Remote Support, VPN, and Docs |
| 8.21 | 24 April 2023 | "Android 8.21 Release Notes" on page 38 | Core, Secure Browser |
| 8.20 | 2 April 2023 | "Android 8.20 Release Notes" on page 38 | Core |
| 8.15 | 13 February 2023 | Android 8.15 Release Notes | Core |

## MaaS360 for iOS

** iOS apps that are available on iTunes must be reviewed and approved by Apple. Submission dates specify when the app was submitted to Apple. The app is typically released on iTunes 3 to 7 days after the submission date.

| Release Version | Release Date | Release Details |
|---|---|---|
| 5.61 | 20 November 2023 | iOS 5.61 Release Notes |
| 5.60 | 05 September 2023 | “iOS 5.60 Release Notes” on page 40 |
| 5.50 | 28 June 2023 | “iOS 5.50 Release Notes” on page 41 |
| iOS Secure Browser 3.92 | 28 June 2023 | “iOS Secure Browser 3.92 Release Notes” on page 41 |
| iOS Secure Editor 3.30 | 28 June 2023 | “iOS Secure Editor 3.30 Release Notes” on page 41 |
| PIV-D 1.50 | 28 June 2023 | “MaaS360 PIV-D App 1.50 Release Notes” on page 41 |
| 5.41 | 24 April 2023 | “iOS 5.41 Release Notes” on page 41 |
| iOS SDK and Wrapping 4.45 | 17 April 2023 | “iOS SDK and Wrapping 4.45.000 Release Notes” on page 42 |
| 5.40 | 02 March 2023 | iOS 5.40 Release Notes |

## MaaS360 for macOS

| Release Version | Release Date | Release Details |
|---|---|---|
| macOS Agent 2.52.000, App Catalog 1.59.100, and App packager 1.49.100 | 18 October 2023 | macOS Agent 2.52.000, App Catalog 1.59.100, and macOS App packager 1.49.100 |
| macOS Agent 2.49.000, App Catalog 1.58.000, and macOS App Packager 1.48.000 | 24 January 2023 | “macOS Agent 2.49.000, App Catalog 1.58.000, and macOS App Packager 1.48.000” on page 43 |
| macOS Agent 2.50.000, App Catalog 1.59.000, and macOS App Packager 1.49.000 | 30 March 2023 | “macOS Agent 2.50.000, App Catalog 1.59.000, and macOS App Packager 1.49.000” on page 42 |

| Release Version | Release Date | Release Details |
|---|---|---|
| macOS Agent 2.50.100 | 12 May 2023 | “macOS Agent 2.50.100 Release Summary” on page 42 |

## MaaS360 Beta Program

This section lists the MaaS360 apps that are available for Beta testing. If you want to subscribe to the Beta programs, follow the processes that are documented in the following links:

- iOS Beta - How to subscribe
- Android Beta - How to subscribe

| App | Beta App Version | Beta Start Date | Beta Status | Beta Details |
|---|---|---|---|---|
| Cloud Extender | 3.000.700 | 01 February 2024 | OPEN | “Cloud Extender 3.000.700 Release Notes” on page 28 |
| iOS | 5.70 | 30 January 2024 | OPEN | “iOS 5.70 Release Notes” on page 39 |
| Android app | 8.41/8.40 | 06 December 2023 | CLOSED | Android 8.40 Release Notes |
| Android app | 8.35 | 11 October 2023 | CLOSED | “Android 8.35 Release Notes” on page 35 |
| iOS app | 5.60 | 29 August 2023 | CLOSED | “iOS 5.60 Release Notes” on page 40 |
| Android app | 8.30 | 07 August 2023 | CLOSED | “Android 8.30 Release Notes” on page 35 |
| PIV-D app | 1.50 | 16 June 2023 | CLOSED | “MaaS360 PIV-D App 1.50 Release Notes” on page 41 |
| iOS Secure Editor | 3.30 | 26 May 2023 | CLOSED | “iOS Secure Editor 3.30 Release Notes” on page 41 |
| iOS Secure Browser | 3.92 | 26 May 2023 | CLOSED | “iOS Secure Browser 3.92 Release Notes” on page 41 |
| iOS app | 5.50 | 26 May 2023 | CLOSED | “iOS 5.50 Release Notes” on page 41 |
| Android app | 8.26 | 13 June 2023 | CLOSED | Android 8.26 Release Notes |
| Android app | 8.25 | 22 May 2023 | CLOSED | “Android 8.25 Release Notes” on page 36 |
| Android app | 8.21 | 17 March 2023 | CLOSED | “Android 8.21 Release Notes” on page 38 |
| Android app | 8.20 | 13 March 2023 | CLOSED | “Android 8.20 Release Notes” on page 38 |
| iOS app | 5.40 | 02 March 2023 | CLOSED | iOS 5.40 Release Notes |
| Android app | 8.15 | 07 February 2023 | CLOSED | Android 8.15 Release Notes |

# Cloud Release Notes

MaaS360 Cloud Release Notes

## What's New Since 10.90 Release Notes

List of features and enhancements introduced after the release of MaaS360 Cloud version 10.90.

### Version 10.90.cd.09022024 Released 09 February 2024

**Automatic activation of Samsung Knox Platform for Enterprise (KPE) premium licenses through MaaS360 portal >>**

Samsung makes Knox Platform for Enterprise (KPE) premium licenses available to customers at no additional cost. A Premium license is required to unlock advanced configurations for Knox devices such as Allow dual SIM operation, Allow remote control, and Allow bluetooth scanning. Previously, administrators had to manually obtain and deploy KPE premium license keys through the MaaS360 portal. MaaS360 eliminates that step in this update by automatically embedding EMM-specific premium license keys directly within the Samsung OEMConfig profile. When administrators republish the OEMConfig, Samsung automatically activates these hidden keys on enrolled Samsung devices. For customers who already purchased KPE premium licenses through Knox resellers, the option to deploy those keys through the MaaS360 portal remains available. Importantly, keys obtained from resellers will take precedence over the EMM-specific ones, ensuring continued access to their chosen license configuration.

For more information about KPE license keys, contact Samsung Knox support team.

**Customize the error message shown to users when devices do not meet OS requirements >>**

In previous releases, MaaS360 introduced an advanced enrollment setting Enroll under Android for Enterprise only if the OS version is above, enabling administrators to set minimum OS version requirements for Android Enterprise enrollments. If devices fail to meet the criteria during enrollment, a generic error message is displayed and the enrollment is blocked. In this release, MaaS360 adds a new branding element to tailor error messages displayed to users when their devices don't meet the minimum OS requirement for Android Enterprise enrollment. Administrators can use this feature to provide a custom message that allows users to understand the issue and potentially take corrective actions, such as updating their device OS or exploring alternative enrollment options.

**Note:** Path to the new branding element: **Setup** > **Branding** > **Branding Elements** > **Android Enrollment Configuration** > **Error message if minimum allowed version criteria are not met**.

### Version 10.90.cd.19012024 Released 19 January 2024

**Support TLS 1.3 protocol**

NIST announces the publication of NIST Special Publication (SP) 800-52 Revision 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations.

To adhere to FedRAMP and NIST Special Publication compliance, the MaaS360 Portal will provide support for the TLS 1.3 protocol beginning in January 2024.

In addition to the currently supported TLS 1.2 cipher suites, the newly added TLS 1.3 cipher suites are as follows:

- TLS_AKE_WITH_AES_128_GCM_SHA256
- TLS_AKE_WITH_AES_256_GCM_SHA384
- TLS_AKE_WITH_CHACHA20_POLY1305_SHA256

For information about all the ciphers supported in Maas360, see MaaS360 platform system requirements.

### Version 10.90.cd.21122023 Released 21 December 2023

**Enhanced Android Enterprise enrollment options in MaaS360 Portal**

MaaS360 adds a major update to the Android Enterprise enrollment options within the MaaS360 portal. This update includes a reorganized interface that simplifies the management of Android Enterprise enrollments, offering a more intuitive experience for administrators.

Key enhancements in the new user interface:

- **Restructured enrollment settings**: The enrollment settings are now neatly categorized by platform (Android, iOS, Windows) under **Devices** > **Enrollments** > **Other Enrollment Options**. The enrollment settings are now logically grouped under corresponding sections. For instance, Android enrollment options are located under the Android section, eliminating the previous grouping of options for all platforms (iOS, Android, Windows) in a single menu.
- **New Android enrollment wizard**: MaaS360 adds a new wizard which is accessible in **Devices** > **Enrollments** > **Other Enrollment Options** > **Android**. This new wizard centralizes enrollment configuration options for all Android Enterprise methods. Administrators can now easily configure Android enrollments in one place, eliminating the need for multiple workflows. Additionally, MaaS360 introduced a dedicated option in the Android enrollment wizard for generating KME Device Owner enrollment configurations. In the previous releases, administrators had to use Zero-touch enrollment option to generate JSON configuration for KME Device Owner enrollments.

For more information about Android Enterprise enrollment options and modes, see Android Enterprise enrollment guide

## Version 10.90.cd.11122023 Released 11 December 2023

### Decommissioning of BlackBerry Details report >>

In December 2023, MaaS360 decommissions the BlackBerry Details report in the MaaS360 Portal. This update is implemented to optimize the portal's functionality, considering the reduced usage of these reports.

### Decommissioning of PC Overview report >>

In December 2023, Maas360 decommissions the PC Overview report in the MaaS360 Portal. This update is implemented since all the metrics and statistical data presented in the PC Overview report are included in the UEM Overview reports, which are accessible to all users by default.

## Version 10.90.cd.07122023 Released 07 December 2023

### Introducing risk rule and risk scoring for vulnerable third-party applications >>

The Application security risk rule is introduced in the Risk Rule Configurator and is enabled by default for customers who have enabled the Risk Based Application Patching service in the MaaS360 Portal. This rule assesses the application security posture of devices. MaaS360 creates risk incidents when app vulnerabilities are detected and then validates them against the risk rule to calculate the severity and risk score for devices and users.

## Version 10.90.cd.08112023 Released 08 November 2023

### Actions Log to track status of security actions >>

MaaS360 introduces an Actions Log page to track the status of security actions taken by administrators within an organization. These actions are taken on devices and logical groups to restrict risky users and devices from gaining unauthorized access to corporate resources. The security actions include remediation actions, such as upgrading applications, uninstalling applications, and notifying devices. The page displays the action log data for the past 6 months.

For information on tracking the status of security actions taken in the Application security dashboard, see Application security widget and Remediating vulnerable apps.

**Note:** This feature is not generally available. You must contact IBM Support to get this feature enabled for your account.

### Version 10.90.cd.03102023 Released 03 October 2023

**Support for remediation action in the Application security widget >>**

MaaS360 has enhanced the Application security offering in the Security Dashboard to introduce a new remediation capability. Administrators can use the remediation action to update or uninstall vulnerable third-party apps installed on devices. This action can be performed on a single device, multiple devices, or all devices. Administrators can also send notifications to users and devices about app vulnerabilities.

**Note:**

- The Risk Based Application Patching offering is currently available for non-federal customers only. This offering is not available to federal customers until FedRAMP approval is obtained for the required services.
- This feature is not generally available. You must contact IBM Support to get this feature enabled for your account.

### Version 10.90.cd.22092023 Released 22 September 2023

**Support for new Zebra OEMConfig app >>**

MaaS360 adds support for the new Zebra OEMConfig Powered by MX app, a new version for Zebra devices running Android 11 and Android 13 and later. This app delivers numerous enhancements built by Zebra, including an all-new schema designed according to changes mandated by Google.

To use the new Zebra OEMConfig app, you must:

1. Create an OEMConfig profile in the MaaS360 Portal using the new Zebra OEMConfig Powered by MX app.
2. Distribute the profile to Android 11 and Android 13+ devices.

For more information on using OEMConfig apps in MaaS360, see https://www.ibm.com/docs/en/maas360?topic=security-using-oemconfig-apps-apply-advanced-device-configuration-policies-in-maas360

**Note:** The new version is not compatible with Android 10 or older Android versions.

## Release Notes for 10.90

List of features and enhancements that are introduced in MaaS360 Cloud version 10.90.

### Portal

**Support to import and export MDM policy settings in the MaaS360 portal >>**

Administrators can now seamlessly export MDM policies from one MaaS360 account and import them into another. This feature makes it easier for customers handling multiple MaaS360 sandbox and production accounts for different business units to maintain uniform policy settings across all accounts.

**Extended the Notify action in Security Dashboard to Windows devices >>**

MaaS360 makes the Notify action available for Windows devices, allowing administrators to send notifications about risk incidents to these devices from the Security Dashboard. In the previous releases, MaaS360 added the Notify action support for Android and iOS devices.

### Android

**Granular reporting for Kiosk mode status >>**

MaaS360 introduces granular reporting for Kiosk mode status. The Device Summary page now displays detailed kiosk failure states from both the MaaS360 agent and kiosk apps. The newly added kiosk state labels provide a clear distinction between kiosk failure states (**Error**: Download failed) and kiosk exit states (**Exited**: via Admin action). Administrators can use Advanced Search to filter devices based on these new kiosk states. Additionally, MaaS360 enhances logging to enable administrators to collect detailed failure state information from affected devices. This update addresses multiple defects in devices, where either the Kiosk mode was not applied, or devices exited Kiosk mode upon reboot. Furthermore, MaaS360 evaluates kiosk status during every policy evaluation and attempts to reapply kiosk settings in scenarios where the kiosk exits randomly without a known reason.

Advantages:

- Collects precise failure state information for quicker and more accurate troubleshooting.
- Provides better awareness of the exact kiosk status on devices.
- Saves time in reviewing kiosk-related issues.

**Note**: The device groups created with the old Kiosk mode status in your MaaS360 account are no longer valid. For example, in the new enhancement, MaaS360 has divided the Exited state into granular states. Therefore, administrators must redefine advanced search conditions based on the new Kiosk mode statuses.

### Android 14 zero-day support >>

MaaS360 announces zero-day support for Android 14. With this support, new Android 14 devices that are enrolled in MaaS360 and existing devices that are upgrading to Android 14 continue to work seamlessly without disruption. MaaS360 ensures that both IT and end-users can take advantage of the new features that are built into Android's updated operating system from the day of release.

### Behavior changes

When MaaS360 runs on Android 14, there will be behavior changes that impact some of the features in the MaaS360 app.

- **Schedule exact alarms permission is denied by default >>**

  SCHEDULE_EXACT_ALARM is no longer pre-granted to apps targeting Android 13 and higher. If an existing app already had this permission, it'll be pre-granted when the device upgrades to Android 14. MaaS360 introduces a new tab **New Permissions** which displays the permissions required by the new version of the MaaS360 app. When users upgrade to MaaS360 for Android app version 8.30, the MaaS360 app now presents the list of mandatory permissions, including **Alarms & reminder**, enabling users to easily view and grant the permissions required by the MaaS360 app.
- **Discontinued support for new Device Admin enrollments >>**

  Starting from Android OS version 14, MaaS360 discontinues support for Device Admin enrollments. If users try to enroll Android 14 devices in Device Admin mode, MaaS360 will display an error message and block the enrollment process. However, devices that are already enrolled in Device Admin mode will continue to function properly when they are upgraded to Android 14.

### Apply custom wallpaper and lock screen configuration for shared devices >>

MaaS360 automatically applies the wallpaper and lock screen configurations from the default Android MDM policy when the shared device is in a selective wipe or signed-out state. Administrators can leverage wallpaper and lock screen configurations to show contact numbers or custom text, such as sign-in instructions. In the previous releases, MaaS360 removed all configurations including the wallpaper and lock screen configurations from the shared device on selective wipe and sign-out.

### Simplified Android Enterprise integration in MaaS360 >>

MaaS360 adds minor user interface enhancements to the Mobile Device Management service, making it easier for administrators to set up Android Enterprise in the MaaS360 Portal. Once linked to an Android Enterprise account, MaaS360 indicates the connection status with a **Connected** label with a green tick mark. If administrators want to disconnect the Android Enterprise account, they can click the **Discontinue** button instead of clearing the **Enable Android Enterprise Solution set** checkbox.

### Enhanced Reset Passcode Interface in MaaS360 Portal >>

When resetting the passcode through the device-level **Reset Passcode** action, MaaS360 displays the Passcode Complexity level for Android 12+ devices. This enhancement allows administrators to set the passcode based on the passcode policy settings that are currently applied to the devices.

## iOS

### iOS 17 zero-day support >>

MaaS360 announces same-day support for iOS 17. With this support, new iOS 17 devices enroll with MaaS360 and existing devices upgrading to iOS 17 continue to work seamlessly without any disruption.

### Advanced iOS supervised policy settings >>

MaaS360 introduces new supervised policy settings and deprecated some of the existing policy settings for iOS 17 devices.

### New DEP enrollment Skip Items >>

MaaS360 adds new Skip Item panes in the Add Profile workflow of DEP (Device Enrollment Program). Administrators can now customize the enrollment process by letting users skip the Safety, Intended User, and Terms of Address panes.

### Enhancements to the Push OS Update command >>

MaaS360 added new features that simplify the OS update process and ensure that devices are always running the selected OS version with the necessary security enhancements.

MaaS360 adds the **Latest Version** option in the Select OS Version menu for the group action. When this option is selected, MaaS360 automatically deploys the most recent OS version applicable to each device model. In the previous releases, administrators had to manually identify and apply the latest OS version that was compatible with each device model.

### Deploy Rapid Security Responses (RSR) through MaaS360 Portal >>

Administrators can now use the Push iOS Update action to remotely deploy Rapid Security Responses (security patches) to iOS devices. When deploying OS updates, MaaS360 displays the complete list of software versions and RSR versions that are currently supported by Apple.

**Note**: The Rapid Software Response (RSR) versions are displayed in both device level and group actions. New Rapid Security Responses are delivered only for the latest versions of iOS and are compatible only with the corresponding base OS versions.

### Certificate-based authentication for the Extensible Single Sign-On Kerberos >>

MaaS360 now supports certificate-based authentication for the Extensible Single Sign-On Kerberos. To perform certificate-based authentication, administrators must select a user-level certificate template in the Identity Certificate field in the Kerberos Extensible Single Sign-On policy settings. If administrators do not select a certificate, MaaS360 uses credential-based authentication wherein the users are prompted to provide the username and password of the user.

**Prerequisite**: User certificate templates must be configured on Cloud Extender.

## macOS

### macOS 14 Sonoma zero-day support >>

MaaS360 announces same-day support for macOS 14. With this support, new macOS 14 devices enroll with MaaS360, and existing devices upgrading to macOS 14 continue to work seamlessly without any disruption. MaaS360 also adds new policy restrictions that are introduced with macOS 14 Sonoma. For a detailed list of macOS 14 functionality restrictions, see macOS 14 Sonoma restrictions.

### Enhancements to the Push macOS Update command >>

Administrators now have more control over updating macOS devices to specific versions. Instead of automatically updating to the latest OS version, administrators can now select the desired macOS version from available options in the MaaS360 portal. Additionally, MaaS360 introduces the **Latest Version** option in the Select OS Version menu for the group action. This option automatically deploys the most recent macOS version applicable to each device model.

**Note**:

- The device action displays OS versions based on the device's current macOS version and model number. For the group action, MaaS360 presents a static list of macOS versions currently supported by Apple.
- MaaS360 does not install the macOS version if it is incompatible with the device model or if the device is already running a newer software version.
- Supported on macOS devices running 11 Big Sur and later.

**Enhancements to the Restart Mac command >>**

MaaS360 now adds the ability to notify users before restarting the devices. When administrators select the **Notify User** option in the Restart Device action, MaaS360 notifies the user to restart the device at their preferred time. A forced restart will only occur if the device is at the login window with no logged-in users. The user can dismiss the notification and ignore the request. No further notifications are displayed unless administrators resend the command.

**Improved FileVault Recovery Key Management for macOS Devices >>**

When a macOS device is enrolled, the device generates a FileVault recovery key which is retrieved by MaaS360. If users forget their Mac login password, they can use the recovery key to unlock the disk and reset their password. However, if the macOS device is wiped or re-enrolled, the existing FileVault recovery key is rendered invalid. To address this issue, MaaS360 now allows administrators to create a smart group of re-enrolled devices with outdated recovery keys and then issue the group-level action **Escrow FileVault Recovery Key** to regenerate the recovery key for those devices.

## What's New Since 10.89 Release Notes

List of features and enhancements introduced after the release of MaaS360 Cloud version 10.89.

### Version 10.89.cd.21072023 Released 21 July 2023

**New Application security widget to view top vulnerable apps in an organization >>**

MaaS360 adds the new Application Security widget in the Security dashboard. This widget provides a comprehensive overview of all vulnerable 3rd party apps and vulnerabilities detected in applications deployed across an organization. Using this widget, you can uncover new and historical CVE information associated with the 3rd party application, and review its impact on your enterprise.

This service also highlights applications affected by security vulnerabilities while providing an overview of the app’s security assessment. The detection workflow provides actionable intelligence and increases the efficiency and ease with which you maintain a secure app environment.

**Note:**

- The Risk Based Application Patching offering is currently available for non-federal customers only. This offering is not available to federal customers until FedRAMP approval is obtained for the required services.
- This feature is not generally available. You must contact IBM Support to get this feature enabled for your account.

### Version 10.89.cd.15062023 Released 15 June 2023

**Fixed MaaS360 Wi-Fi Configuration issue on Android devices >>**

Wi-Fi profiles using 802.1x EAP with certificates failed to deploy to Android 13 devices with the latest security patches. As a result, the Wi-Fi profiles were stuck in the Pending state on the Settings page of the MaaS360 for Android app.

MaaS360 added two text fields in the Wi-Fi section of the Android Enterprise MDM policy. These fields are displayed only when the **802.1x EAP** has been set as the **Wi-Fi configuration** type. To successfully deploy the Wi-Fi profile on devices, it is essential to configure one of the following two settings in the Wi-Fi profile. For more details about these settings, see https://www.ibm.com/docs/en/maas360?topic=cpsaed-wi-fi.

**Note:** This fix requires MaaS360 for Android app version 8.26.

## Version 10.89.cd.02062023 Released 02 June 2023

### Streamlined enrollment process to install apps on newly enrolled devices without delays

When enrolling a new device, MaaS360 now sets the policy in the background before adding the managed Google Play Account to the device. This change addresses a previous issue where the policy was applied after enrollment, leading to the failure of auto-installing Managed Google Play apps on devices. This enhancement streamlines the device onboarding process and ensures that the desired apps are automatically installed on enrolled devices without any manual intervention.

**Note:** This enhancement does not introduce any behavior or UI changes. The updates are implemented seamlessly in the background, requiring no action from users.

### MaaS360 now uses the latest Apktool for wrapping

MaaS360 uses Apktool, an open-source library tool for Android app wrapping. The MaaS360 portal is now enhanced to use the latest Apktool version 2.7.0.

The latest version of ApkTool adds the following improvements:

- Support for API 33.
- Enhanced support for AndResGuard / Proguard resource tricks.
- Correct compression handling with remapped resources.
- Enhanced support for applications with multiple styles res types.

## Version 10.89.cd.13052023 Released 31 May 2023

### General availability of policy modernization enhancements to macOS customers >>

MaaS360 announces the general availability of the Policy Modernization framework for macOS devices. This release introduces a new and improved user interface (UI) for managing policies on macOS devices, enhancing the overall policy management experience.

Existing MaaS360 customers will receive access to the modernized UI through a phased rollout, ensuring a smooth transition and seamless integration with their existing workflows. For new MaaS360 accounts, the Policy Modernization framework is available by default. For more information about policy modernization, see https://www.ibm.com/support/pages/node/6562435.

## Version 10.89.cd.31052023 Released 31 May 2023

### Specify a specific iOS version when issuing an OS update command to iOS devices >>

MaaS360 now allows administrators to update devices to a specific iOS version by selecting the desired version from the available options in the MaaS360 portal. With this support, administrators can have granular control over the iOS update process and ensure consistency across managed devices by selecting a specific iOS version to be installed. By deploying older OS versions on a subset of devices, administrators can test the compatibility of their organization's apps, software, and systems with the new iOS version before fully adopting it. In the previous releases, administrators could deploy the latest software update only.

**Note:** The list of supported OS updates displayed in the MaaS360 portal varies based on the iOS version currently installed on iOS devices.

### Support for new quarantine action in Security Dashboard >>

MaaS360 adds the quarantine action in the Security Dashboard to restrict risky users and devices from gaining unauthorized access to your corporate resources. The Quarantine action ensures that only trusted users and devices can access Single Sign-On apps in your organization. You can apply the quarantine action to users from the Security Dashboard based on their risk score and risk level. When this action is enforced, users are restricted from accessing SSO-enabled apps or prompted to provide additional authentication factors to verify their identity until the quarantine is lifted.

## Version 10.89.cd.16052023 Released 16 May 2023

### Support to block self-enrollments for iOS and macOS devices >>

MaaS360 introduces improvements to limit self-enrollments of iOS and macOS devices, ensuring that only enrollments initiated by the administrator or through administrator workflows are permitted. When this feature is enabled, users are blocked from enrolling their BYOD or employee-owned devices using the self-enrollment URL. However, they can still enroll these devices by using the enrollment request URL provided by the administrator.

Enabling this option automatically deactivates all self-enrollment settings associated with BYOD and employee-owned devices on the iOS and macOS platforms.

## Version 10.89.cd.08052023 Released 08 May 2023

### Trial part for License Management enabled customers >>

For customers who want to try out features of MaaS360 outside their subscriptions after License Management is activated, an additional Enterprise Trial part D1P3CTR has been created that is valid on 10 devices for 30 days. Customers can get this trial part provisioned on top of their purchased base bundles to try out features of MaaS360 outside their subscriptions.

To get this trial part provisioned, customers must contact MaaS360 Support or visit https://ibm.biz/maas360csm to connect with the CSM team. For information on provisioning the Enterprise Trial part D1P3CTR in the SSM tool, see https://supportcontent.ibm.com/support/pages/node/6988849https://www.ibm.com/support/pages/node/6988849.

### Enrollment limit settings for License Management enabled customers >>

After License Management is activated for an account, the enrollment limit setting for devices and users at **Setup** > **Settings** > **Directory and Enrollment** > **Basic Enrollment Settings**: **By Account** will be disabled and won’t be visible to the portal administrators or the partners managing as a customer. The Overage settings configured for the account will override the enrollment limit setting.

### Enhancements to the device count on MaaS360 Portal >>

The device count displayed on the MaaS360 Portal Home page is now changed to match the number of devices on the License Overview page for all customers. When clicked on this number, the Device Inventory view will show only devices that are activated, enrolled, and in pending removed control state with licenses assigned (user removed control and mailbox sync’ed devices will not be part of this number).

An administrator landing on the devices view page from Device Inventory menu sees the same count as above. The list will show only actived, enrolled, and in pending removed control state devices. Administrators can apply required filters to view devices in other states.

Devices that are pending control removal will have the licenses removed when the devices receive and apply this action. For devices that did not get the action for a prolonged time for any reason, the administrator can hide such devices which will remove the license from them. Unless hidden, these devices would continue to be included in the device count shown on the MaaS360 Portal Home page.

Previously, the device count included devices that were enrolled and not enrolled in the MaaS360 Portal, active, synced, devices where the user removed control of the device, or devices that are pending a control removal.

### Automatically revoke licenses from devices that move to hidden or inactive state >>

When devices become inactive or move to hidden state, the licenses that are assigned to these devices are automatically revoked. Devices without licenses are not accounted for billing. Whenever a device moves back from hidden to active state, the licenses are auto-assigned to the device in a certain order of priority.

## Version 10.89.cd.03052023 Released 03 May 2023

**Policy modernization enhancements >>**

MaaS360 announces the general availability of the new policy modernization framework for iOS, Android, and Windows platforms. This means that all MaaS360 accounts (new and existing) will have the latest policy modernization framework enabled by default. In the redesigned framework, MaaS360 simplifies the user experience, improves performance, and adds significant enhancements to policy configuration, policy assignment, review changes, policy audit, and bulk update workflows. https://www.ibm.com/support/pages/node/6562435

**Note:** Policy Modernization enhancements are not available by default for the macOS platform. Contact the MaaS360 Support team to get the macOS policy modernization framework enabled for your account.

The modernized framework makes it easier for administrators to:

- Track the policy distribution status and re-push the policy if the policy failed to apply to devices.
- Apply policy settings to multiple policies at once through the bulk update feature.
- Upload policy files such as certificates, images, and custom OMA settings to devices.
- Track policy distribution status on the device History page.
- Resolve conflicts when multiple profiles are assigned to the same device through group distribution.

**Automatically processing the orphaned threat management data for cleanup >>**

MaaS360 will now automatically clean up system-stored data when administrators perform the following activities:

- Disable a risk rule
- Delete a device record
- Turn off User Risk Management or Threat Management service

For example, if administrators turn off the Malware detection risk rule, MaaS360 automatically deletes the corresponding threat activity data such as risk severity, risk score, Security Dashboard reports, and device view summary from the MaaS360 portal. MaaS360 will not restore events and violations that are processed for cleanup. If administrators re-enable the risk rule, MaaS360 uses that rule to validate new risks that occur in the future**.**

**Note**

- The data is permanently deleted from the MaaS360 portal. To comply with GDPR standards, MaaS360 will not restore the data that is processed for cleanup.
- The Security Dashboard reports refresh immediately after the clean-up.

### Version 10.89.cd.14042023 Released 14 April 2023

**Non-silent notification support for Secure Mail for iOS app >>**

Administrators can now enable non-silent notifications for the Secure Mail app. Non-silent notifications ensure that iOS devices receive notifications for Inbox activities even though the Secure Mail app is not running in the background or the device is locked.

### Version 10.89.cd.03042023 Released 03 April 2023

**Support activation of License Management for MaaS360 customer accounts >>**

- MaaS360 provisions self-serviceable activation of license management.

  Note: This feature is not generally available. You must contact IBM Support to check for eligibility and get this feature turned on for your account. Once available, portal administrators can activate license management for their MaaS360 accounts. After activation, all the license management features will become available.
- To activate license management for business partner accounts, you must contact IBM Support.

- License management can be enabled for direct and non-ESA partner customers with device-based or user-based licenses.

**Restrict usage of services that are not subscribed >>**

MaaS360 restricts the usage of services that are outside the purchased license suites. All devices using these excess services will lose the entitlements 90 days after activation of license management for an account. You must purchase the licenses for the excess services to continue using the license within those 90 days. **Note:** Contact MaaS360 Sales or your Customer Success Manager to purchase the Base or Add-on licenses. You can also visit https://www.ibm.com/products/maas360/pricing to purchase Base licenses.

**Enhancements to License Settings UI >>**

The License settings UI has been redesigned to facilitate the configuration of Overage Settings, Auto-assignment of licenses for self-enrollments and self-activations, and Alert settings related to license management on a single UI screen.

**Version 10.89.cd.29032023 Released 29 March 2023**

**Track the policy distribution status for devices >>**

Administrators can view all the devices that are in scope for a policy and track the policy distribution status for those devices at a granular level. This feature is supported for iOS, Android, and Windows devices.The Re-push policy remediation action has been introduced to re-push a policy if the policy failed to apply to devices or is partially delivered to devices.

**Note:** You must use this action with caution since the entire policy (including all the related configurations) is applied to the device again. This may cause payloads to reload on the device and re-requests for the certificates if any are configured.You can view the current policy distribution status of a device on the Device history page and Actions and Events page for devices in the MaaS360 Portal.

# Release Notes for 10.89

List of features and enhancements that are introduced in MaaS360 Cloud version 10.89.

## Portal

**Show text type custom attributes during enrollment >>**

Administrators configure enrollment settings in the MaaS360 Portal to display custom attributes for users on the device enrollment screen. After the enrollment, administrators can track the input provided by users against those custom attributes on the Device Summary page in the MaaS360 Portal.

In the previous releases, MaaS360 supported custom attributes of type Boolean and Enum in **Settings** > **Advanced Enrollment Settings** > **Show Custom Attributes During Enrollment**. Effective with 10.89, MaaS360 adds support to show text type custom attributes during enrollment.

**Note:** The **Show Custom Attributes During Enrollment** setting is not available to all customers by default. Administrators must contact the MaaS360 support team to get this setting enabled for their accounts.

## iOS

**Per App VPN support for PIV - D >>**

MaaS360 adds per-app VPN support for organizations using Derived (PIV) Credentials with MaaS360. With this support, administrators can configure the list of managed apps that use the secure VPN connection. When the VPN profile reaches the device, MaaS360 allows only configured apps to use the VPN tunnel. When users open the app, it automatically connects to the VPN and routes the traffic through the VPN tunnel. When the app is inactive, the VPN is not used.

**Prerequisite**: Customers must have the Derived Credential service enabled in the MaaS360 portal.

**Track secondary SIM information in Device Summary >>**

iOS models that support dual SIMs will now report secondary SIM details to the MaaS360 Portal. In the previous releases, MaaS360 displayed only primary SIM details of iOS devices that used a physical nano-SIM. With this support, administrators can view secondary SIM details in the MaaS360 portal and easily filter devices in their organization using the secondary SIM information such as Phone Number, ICCID, and IMEI.

The primary and secondary SIM details are displayed in the following path: **Devices** > **Inventory** > **View** > **Summary** > **Network Information**.

**Note:**

- Secondary SIM information is displayed only if devices use two SIMs (Nano-SIMs, eSIMs, or a combination of both). The Secondary SIM information is unavailable if the device uses only one physical nano-SIM.
- If users activate an eSIM and leave the physical SIM tray empty, MaaS360 displays eSIM details in the Secondary SIM Details section.

## Android

### Support to exclude the Notification permission when configuring runtime permission using the All option >>

When configuring default runtime app permissions, administrators use the All option to grant or deny all permissions for an app at once. Effective 10.89, MaaS360 allows admins to exempt the Notification permission when the All option is selected.

### Support for System Update policies for Work Profile on Corporate Owned (WPCO) devices >>

MaaS360 extends System Update policies to WPCO devices. Administrators can use these policies to configure when over-the-air system updates are installed on a device. This policy affects the pending system update (if there is one) and any future updates for the device. In the previous releases, these settings were supported only on Device Owner devices.

**Note:**

- If a policy is set on a device, the system doesn't notify the user about updates.
- Supported only on Android 11+ (WPCO) devices.
- Requires MaaS360 for Android app version 8.20+.

## macOS

### New device-level actions to remotely restart and shut down macOS devices >>

MaaS360 adds two real-time MDM device-level actions to allow administrators to remotely restart and shut down managed macOS devices from the MaaS360 portal.

**Note:**

- The Restart device command is supported on macOS 11.3+ devices. The Shutdown device command is supported on macOS 10.13+ devices.
- These commands automatically turn off devices as soon as the command reaches those devices. Any unsaved work will be lost.

### Support for advanced macOS profiles >>

**Extensible Single Sign-on (SSO) policy**: Administrators can use this payload to configure an app extension that performs single sign-on (SSO). This payload streamlines the login experience for users logging into apps and websites through third-party identity management providers (IdPs) such as PingOne, IBM Security Verify, and Microsoft Azure AD. When properly configured using MDM, the user authenticates once and then gains access to subsequent native apps and websites automatically. **Note**: Supported only on macOS 10.15+ devices.

**Privacy Preferences Policy Control (PPPC) policy**: Administrators can remotely manage the security preferences in the Privacy pane of Security & Privacy preferences of the device. To protect the end user's privacy, macOS 10.14+ devices require users to explicitly allow apps to access privacy features such as Photos, Calendar, Accessibility, Camera, and Microphone. The PPPC policy settings in the MaaS360 portal allow administrators to remotely pre-approve or pre-deny access to these privacy features on behalf of the user. These policy settings override the user preferences configured on the macOS devices. Note: Supported only on macOS 10.14+ devices.

### Threat Management

**Notify users about security incidents by invoking an action from the Security dashboard >>**

MaaS360 adds the Notify action in the Security Dashboard, allowing administrators to send notifications to risky devices and users. Notifications alert users about risk incidents on their devices and help them decide the next course of action to take. The default notification message contains information about the security incidents that are detected on devices. However, administrators can customize the default notification message based on their requirements.

**Prerequisites**: Customers must have the **Threat Management** service enabled in the MaaS360 Portal.

### Platform

**Enhancements to Administrator Audit Reports >>**

The Administrator Audit Reports page that is used to generate audit data reports for the MaaS360 portal administrator workflows is now generally available. You can generate reports for ten different report types for the previous 60 days for a customer account. The reports are generated in CSV file format and sent to the recipient's email address(es) within 30 minutes.

**https://www.ibm.com/docs/en/maas360?topic=maas360-portal-administration-audit-reportsTrack policy distribution progress for devices >>**

MaaS360 tracks the progress of the policy distribution status for devices at a granular level. For the Change Policy action taken on a device, the policy distribution status is displayed on the *Actions and Events* page for devices and the *Device history* page. The statuses include various intermediate stages that are involved in policy distribution. For information on status on the *Actions and Events* page, see https://www.ibm.com/docs/en/maas360?topic=devices-viewing-action-history-events-device.

### Webservices

No APIs were added or updated for this release.

## What's New Since 10.88 Release Notes

List of features and enhancements introduced after the release of MaaS360 Cloud version 10.88.

### Version 10.88.cd.07022023 Released 07 February 2023

**Deprecation of legacy VPP app management APIs >>**

Apple deprecates legacy Volume Purchase Program (VPP) app management APIs in favor of new and advanced VPP app management APIs. The features and improved asynchronous processing in the new app management APIs enable administrators to manage apps in a faster and more scalable way. MaaS360 customers are automatically migrated to the new APIs in a phased rollout without any effort from the administrators. For more information, see https://www.ibm.com/support/pages/node/6953495.

### Version 10.88.cd.13012023 Released 13 January 2023

**Enhanced enrollment request creation mechanism in MaaS360 >>**

MaaS360 added an internal API that returns an enrollment ID in the response. If an enrollment request is available for the user, this API uses that request for enrollment. If an enrollment request is unavailable, this API automatically creates a new request for that user.MaaS360 added the following custom enrollment attribute to allow administrators to troubleshoot DO enrollment issues: **Key**: enrollment_request_mechanism**Value**: parallelEnrollment, useLegacy, or useAdvance

- **parallelEnrollment** - Allows enrollment of multiple devices simultaneously. By default, an enrollment request is used for the enrollment of one device only. If you enroll multiple devices, MaaS360 creates a new enrollment request for each user (or email address specified in the QR/JSON).
- **useLegacy** - MaaS360 uses this value by default if the Authentication Mode for Enrollment is set to Passcode. You must use this value only for the troubleshooting of DO or WPCO authentication issues.
- **useAdvance** - This is the default value. If an enrollment request is already available for the existing user/email ID, MaaS360 uses that enrollment request. If an enrollment request is unavailable, MaaS360 creates a new request automatically in the background.

# MaaS360 Defect Fixes

MaaS360 defect fixes

## December 2023 Daily Fixes Summary

MaaS360 Daily Fixes - December 2023

| Fix | Description | Released |
|---|---|---|
| 46865 | The **View** link was displayed only on the first occurrence of search results using the Global search in the MaaS360 portal. It was disabled for subsequent searches. | 18-Dec |
| 46830 | When the administrator exported MDM policies in Excel file format with policy names containing special characters or languages other than English, the MaaS360 portal saved the file as `download.json` instead of `download.xlsx`. | 06-Dec |
| 46884 | The devices were marked as out of compliance in the MaaS 360 portal due to a mismatch of the rule set when the iOS version was upgraded. | 05-Dec |

## November 2023 Daily Fixes Summary

MaaS360 Daily Fixes - November 2023

| Fix | Description | Released |
|---|---|---|
| 46178 | MaaS360 displayed a graph for data usage analysis reports in the email reports that was inconsistent with the **Data Usage** analysis graph in the MaaS360 portal. | 03-Nov |
| 46877 | The licenses available for the customer account were inconsistent when the number of licenses used (including inactive devices) was compared with the enrolled devices. | 29-Nov |
| 46784 | Administrators were unable to delete the configured App ID in the **App to be Disabled** field for Android MDM policy in the MaaS360 portal. An incorrect title was displayed for the list of configured App IDs. | 29-Nov |

## October 2023 Daily Fixes Summary

MaaS360 Daily Fixes - October 2023

| Fix | Description | Released |
|---|---|---|
| 46685 | After enrolling devices in the userless mode, users were able to add their personal accounts and access the Play Store on those devices. | 25-Oct |

| Fix | Description | Released |
|---|---|---|
| 46649 | After enrolling fully managed, corporate-shared devices in KME mode with a device account, users were unable to sign in to the MaaS360 app. Instead, they received the error message "Failed to link Google account with Play store, click Continue to Sign-out" when signing in. | 20-Oct |
| 46769 | VPP apps failed to install from the App Store on the device even though administrators have appropriate app distributions configured in the MaaS360 portal. | 18-Oct |
| 46272 | When administrators searched for users based on their authentication type in the User Directory page, MaaS360 incorrectly returned only users whose user source was the MaaS360 Directory instead of showing users with all user sources. | 18-Oct |
| 46711 | The error message “Corporate App licensing Setup” was displayed while attempting to install applications on iOS user-enrolled devices, and none of the distributed apps were getting installed on the device through the MaaS360 portal. | 18-Oct |

## September 2023 Daily Fixes Summary

MaaS360 Daily Fixes - September 2023

| Fix | Description | Released |
|---|---|---|
| 46583 | The default profile was not automatically assigned to the newly added DEP devices in the MaaS360 portal. | 01-Sep |
| 46546 | The error message, **The package name is required**, was displayed while attempting to upload an Android enterprise app in the MaaS360 portal. | 03-Sep |
| 46585 | The error message "Managed Apple ID cannot be empty" was displayed when administrators attempted to remove the Managed Apple ID after adding it in the User Summary page. | 06-Sep |
| 46496 | Despite upgrading to the Rapid Security Response version, the Device Summary page and Advanced Search continued to show the base OS version. | 14-Sep |
| 46596 | Administrators were unable to delete inactive devices in bulk. | 14-Sep |
| 46661 | MaaS360 showed a licensing error message, stating "You have a few excess services that will expire," despite the customer no longer using those services. | 15-Sep |
| 46655 | MaaS360 did not support Zebra 13+ devices due to the | 22-Sep |

| Fix | Description | Released |
|---|---|---|
| | unavailability of the new "Zebra OEMConfig Powered by MX" app. | |
| 46710 | In the Device History page, MaaS360 displayed the "??? Pending???" status (with garbled characters) for actions that were pending. | 25-Sep |
| 46708 | Users were unable to connect to the MaaS360 gateway VPN connection configured by administrators in WorkPlace Persona Policies. | 26-Sep |
| 46604 | The devices that joined the group as a result of a group change event did not receive the app configuration. | 28-Sep |
| 46729 | Administrators were unable to clear app configuration checkboxes in MaaS360 once those checkboxes were selected. | 28-Sep |
| 46613 | MaaS360 displayed the error message "Your organization has purchased a limited number of device licenses" when attempting to enroll their devices in the MaaS360 portal. | 29-Sep |

## August 2023 Daily Fixes Summary

MaaS360 Daily Fixes - August 2023

| Fix | Description | Released |
|---|---|---|
| 46533 | Android devices were incorrectly displaying an **Inactive** status, even though they were actively reporting data to the portal. | 11-Aug |
| 46036 | Administrators could not disable the **Windows FileShare MaaS360 Enterprise Gateway** service through Installed Services for iOS devices. | 23-Aug |
| 46261 | Administrators could not clear the activation lock on iOS devices through remote actions. | 28-Aug |
| 46425 | When Android users forwarded an email using Respond Inline in Secure Mail, the recipients received attachments that were 0 KB in size. | 28-Aug |

| Fix | Description | Released |
|---|---|---|
| 46599 | The VPP License assignment page exported blank CSV/Excel files. | 29-Aug |
| 46310 | Resolved the disparity between the security patch level timestamp value displayed on the Advanced Search page and the timestamp displayed on the device-view page. | 29-Aug |
| 46528 | The User Risk Management service was grayed out, preventing administrators from activating it. | 31-Aug |

## July 2023 Daily Fixes Summary

MaaS360 Daily Fixes - July 2023

| Fix | Description | Released |
|---|---|---|
| 46257 | Administrators that do not have the Service Administrator role enabled were unable to view the License field in the Add Device workflow which caused enrollments to fail. | 06-July |
| 46440 | Users could not access emails via the native mail client after configuring email settings in the MDM policy. | 07-July |
| 46392 | An error message was displayed when the primary administrator tried to add new administrators to the MaaS360 portal. | 10-July |
| 46402 | The compliance status of some devices did not sync with Azure AD | 12-July |
| 46368 | The error message "Bundle is not compatible with device platform" was displayed during the bulk license assignment. | 19-July |
| 45976 | The **equal to** condition did not fetch any data for the **Verizon** string in the MaaS360 portal. This issue was caused by an extra space in the **Verizon** string. | Android 8.30 |
| 46360 | All users listed in the Azure AD group were not synced to the MaaS360 User Directory. | 26-July |
| 46494 | MaaS360 displayed a license limit error preventing users from | 27-July |

| Fix | Description | Released |
|---|---|---|
| | enrolling devices, even though enough licenses were purchased and overage was allowed. | |
| 46486 | Administrators were unable to configure the identity and access management settings for Administrator Login. | 27-July |

## June 2023 Daily Fixes Summary

MaaS360 Daily Fixes - June 2023

| Fix | Description | Released |
|---|---|---|
| 46152 | The Administrative Access Control (AAC) option is disabled and cannot be cleared in certain user groups, even though those groups do not have active administrators or distributions enabled for AAC. | 02-June |
| 46141 | Licenses were consumed by inactive devices. When the administrator attempted to track the list of inactive devices, the MaaS360 portal became unresponsive and failed to load. | 05-June |
| 46192 | Some devices lost the ability to detect Wi-Fi connections after a new policy with the setting "Enforce usage of only MDM configured Wi-Fi = No" was applied to those devices. | 07-June |
| 46197 | An error message was displayed when the administrator tried to delete a custom attribute. | 07-June |
| 46325 | Wi-Fi profiles using 802.1x EAP with certificates failed to deploy to Android 13 devices with the latest security patches. | 13-June |
| 46171 | An error message was displayed when the administrator tried to add a public app from the Google play store to the MaaS360 App Catalog. | 16-June |
| 46355 | After configuring Azure AD integration, administrators were unable to sync users to the selected Azure AD groups. | 20-June |

| Fix | Description | Released |
|---|---|---|
| 46154 | Inaccurate event data was displayed on the View Change History page. | 20-June |
| 46208 | The bulk device attribute change failed on the portal when the language was set to Japanese. | 21-June |
| 46363 | After performing the bulk delete operation, administrators did not receive a deletion report as expected. | 21-June |

## May 2023 Daily Fixes Summary

MaaS360 Daily Fixes - May 2023

| Fix | Description | Released |
|---|---|---|
| 45357 | iOS Risk Exposure details were not displayed in the emails received from the MaaS360 portal, despite being shown correctly in the My Advisor section of the portal. | 02-May |
| 46098 | Endpoint Security policies were unavailable in the MaaS360 portal | 04-May |
| 46101 | Android devices entered a state of non-compliance based on the default compliance rule, but the Out of Compliance Reason field did not display the reason for non-compliance. | 05-May |
| 46088 | When the administrator entered a long URL for the Web Clip configuration in the iOS MDM policy, the URL was not correctly reflected in the published Web Clip. | 15-May |
| 46139 | Administrators were unable to publish specific policies. Upon submitting the Publish action, the browser remains in a loading state until it eventually times out without completing the publishing process. | 15-May |
| 46217 | Administrators could not edit the IBM ID and configure a new IBM ID under the Services > Identity and Access Management section. | 16-May |
| 46222 | Policies failed to be applied to iOS Supervised devices after | 16-May |

| Fix | Description | Released |
|---|---|---|
| | enrollment anthe MaaS360 app was not installed on the devices. | |
| 46193 | An app was successfully installed, but the associated app configurations failed to be applied to the device. | 17-May |
| 46013 | An error message was displayed when administrators tried to add an app configuration for the SwiftConnect app through the App Summary page. | 17-May |
| 46235 | The Change Precedence window displayed duplicate OEM Configurations and policy precedence numbers. | 19-May |
| 46054 | The device attestation failed during Device Owner QR code enrollments. | 22-May |
| 45716 | The auto installation of Managed Google Play apps failed on the newly enrolled Device Owner devices. | 31-May |
| 45978 | The Push OS update action was unavailable for some macOS devices in the MaaS360 portal. | 31-May |
| 46164 | The Apple Volume Purchase Program (VPP) page experienced unresponsiveness, preventing administrators from changing their already uploaded VPP token. | 31-May |
| 46071 | The devices containing policy names with 2-byte characters were not displayed in the Advanced Search. | 31-May |
| 46249 | A device license error was displayed when users tried to enroll devices in the Profile Owner mode. | 31-May |

## April 2023 Daily Fixes Summary

MaaS360 Daily Fixes - April 2023

| Fix | Description | Released |
|---|---|---|
| 45838 | MaaS360 displayed inaccurate Minimum OS requirements for macOS applications on the App Summary page. | 04-April |

| Fix | Description | Released |
|---|---|---|
| 45986 | Home screen configuration templates were unavailable for selection in iOS MDM policies. | 05-April |
| 45876 | The Push iOS Update command does not go through. | 06-April |
| 45896 | The EULA agreement was not displayed properly in the MaaS360 for Android app. | 06-April |
| 45419 | When resetting the passcode through the device summary page, an error message was not displayed if minimum passcode requirements were not met. | 07-April |
| 46011 | The new app configurations for the Microsoft Outlook app were not applied to the iOS devices. | 07-April |
| 45911 | iOS policies could not be applied to devices until the Extensible SSO setting was disabled. | 07-April |
| 45899 | The incorrect policy precedence value was displayed on the Policy List view page. | 13-April |
| 45991 | An error message was displayed when administrators tried to apply the Knox Service Plugin(KSP) settings to devices. | 14-April |
| 45989 | An error message was displayed while searching for devices using the Device Type column on the Device Inventory page. | 17-April |
| 46061 | After deleting an existing Identity Provider configuration in IBM Security Verify (ISV), the Identity provider that was newly added in MaaS360 did not reflect in ISV. | 20-April |
| 46112 | MaaS360 could not retrieve device inventory details after enrollment. | 21-April |
| 46084 | Administrators were unable to reset passwords on Android devices through the MaaS360 portal. Path: Device Summary page > More > Reset Passcode. | 21-April |
| 45958 | Administrators were unable to upgrade an Android enterprise app after marking it as Primary. | 24-April |

| Fix | Description | Released |
|---|---|---|
| 46072 | Users were unable to open the MaaS360 App Catalog in the Kiosk mode. | 26-April |
| 45781 | After enrolling devices via afw#maas360 token, users were unable to access Play Store with their Google Workspace account. | 27-April |

## March 2023 Daily Fixes Summary

MaaS360 Daily Fixes - March 2023

| Fix | Description | Release Date |
|---|---|---|
| 45956, 45951, 45993 | If the **Remove on stopping distribution** option was not selected, the web app would remain on devices even though administrators had removed the app in the MaaS360 Portal. | 13-Mar-2023 |
| 45665 | Some devices did not receive the new app update after administrators triggered the app distribution. | 27-Mar-2023 |

## 10.89 Release Fix Summary

The following customer issues were fixed in the 10.89 release:

| Fix number | Description |
|---|---|
| 45821 | Unable to upload .ipa or .apk files to the App Catalog because of special characters in the Description field. |
| 45764 | Spotfire application was crashing when installed with MaaS360. |
| 45717 | Unable to view the My Activity feed updates in the MaaS360 Portal. |
| 45709 | Support icon was broken on Safari. |
| 45670 | Device Group name in Japanese was garbled in the Group Deletion error message. |
| 45650 | Updating an iPad from iOS 15 to iOS 16.1.1 generated an error message "Error.Parsing Request failed," and the device would not update. |
| 45635 | Device inventory wasn't displaying in the MaaS30 Portal. |
| 45590 | Issuing Wifi certificates on mobile devices. |
| 45502 | End User Portal generated Device Admin enrollment requests instead of Profile Owner. |
| 45491 | Unable to access Reports > PC Security > Patches. |

| Fix number | Description |
|---|---|
| 45487 | Mismatch of wording in Android Policy. |
| 45480 | MaaS360 Portal reported incorrect time for last reported devices. |
| 45454 | App configuration user interface was not readable for a long list of package names for the test Android Enterprise app. |
| 45424 | Wi-Fi, AD, and mobile policy settings were not being pushed to macOS devices. |
| 45419 | Console reset passcode was not being flagged immediately as noncompliant until it appeared in the device history. |
| 45336 | Android FRP text was not aligned in the user interface with the field not validating. |

## February 2023 Daily Fixes Summary

MaaS360 Daily Fixes - February 2023

| Fix | Description | Release Date |
|---|---|---|
| 45780 | Registration fails when trying to enable compliance sync with Azure AD for Windows 10. | 01-Feb-2023 |
| 45755 | Administrators could not configure modern authentication for the Outlook app in the App Config. | 03-Feb-2023 |
| 45477 | Administrators could not access the details report in Mobile Data Usage Analysis in MaaS360 Portal. | 10-Feb-2023 |
| 45813 | QR code and Zero-touch enrollments failed sporadically at the Enable real time device ping step. | 15-Feb-2023 |
| 45493 | Administrators could not set up password-less authentication with Cisco IPSEC through VPN policies. | 20-Feb-2023 |
| 45875 | Administrators could not update existing devices with the new app catalog icon image. | 20-Feb-2023 |
| 45848 | The option to bulk delete users was unavailable on the User Directory page. | 22-Feb-2023 |
| 45610 | The Azure AD groups in the MaaS360 Portal disappeared when administrators updated those groups. | 22-Feb-2023 |

## January 2023 Daily Fixes Summary

MaaS360 Daily Fixes - January 2023

| Fix | Description | Release Date |
|---|---|---|
| 45658 | DO enrollments (QR code, KME, and Zero Touch) failed in accounts where the authentication mode for enrollments was set to Passcode. | 12-Jan-23 |
| 45424 | Administrators could not deploy Wi-Fi configurations from the MaaS360 Portal to macOS devices. | 12-Jan-23 |
| 45618 | The Hardware Inventory report was not displayed and the export to .csv was unavailable. | 13-Jan-23 |
| 45707 | The Network Error dialog box was displayed on the PIV-D app. | 19-Jan-23 |
| 45717 | The My Activity Feed home page widget was unavailable for the German locale. | 25-Jan-23 |

# Cloud Extender Release Notes

MaaS360 Cloud Extender Release Notes

## Cloud Extender 3.000.700 Release Notes

List of features and fixes that are released as a part of Cloud Extender3.000.700.

**Upgrade the Cloud Extender installer (core agent), Base module, and the Cloud Extender Configuration Tool to version 3.000.700 or later**

You must upgrade the Cloud Extender to use an enhanced messaging service between Cloud Extender and MaaS360 for better performance and security. For the steps to upgrade, see Upgrading the to use the enhanced messaging service.

**Note:** This upgrade is not generally available. You must contact IBM Support to upgrade your Cloud Extender to 3.000.700.

## Cloud Extender 3.000.400 Release Notes

List of features and fixes that are released as a part of Cloud Extender 3.000.400.

| Fix # | Description |
|---|---|
| 46854 | Cloud Extender Java vulnerability was fixed. |

For details about all the security issues fixed in this release, see https://www.ibm.com/support/pages/node/7115287

### CVE Security Bulletins

The following CVE security bulletin was issued for this release:

| Affected Product(s) | Version(s) | CVE(s) |
|---|---|---|

| | | |
|---|---|---|
| IBM MaaS360 VPN Module | 3.000.300 and prior | CVE-2023-46849,<br>CVE-2023-46850 |
| IBM MaaS360 Mobile Enterprise Gateway | 3.000.100 and prior | CVE-2023-41900,<br>CVE-2023-40167,<br>CVE-2023-36479,<br>CVE-2023-34462,<br>CVE-2023-36478,<br>CVE-2023-44487 |
| Java SDK | 3.000.000 and prior | CVE-2022-40609 |

- Apply the IBM MaaS360 VPN Modules to version 3.000.300 or later.
- Update the IBM MaaS360 Mobile Enterprise Gateway(MEG) to version 3.000.100 or later.

### Resources

To upgrade MEG/VPN modules, see Upgrading the and the modules section.

## Cloud Extender 3.000.300 Release Notes

List of features and fixes that are released as a part of Cloud Extender 3.000.300.

| Fix # | Description |
|---|---|
| 46725 | The identity certificate requests were in pending state when devices were enrolled. |
| 46795 | VPN service was not starting as `.dll` library files were missing. |

For details about all the security issues fixed in this release, see https://www.ibm.com/support/pages/node/7115287

### CVE Security Bulletins

The following CVE security bulletin was issued for this release:

| Affected Product(s) | Version(s) | CVE(s) |
|---|---|---|
| IBM MaaS360 VPN Module | 3.000.200 and prior | CVE-2023-4807,<br>CVE-2023-5364 |

Apply the IBM MaaS360 VPN Modules to version 3.000.300 or later.

### Resources

To Upgrade Cloud Extender Agent and MEG/VPN Modules:

- MEG/VPN: Upgrading the and the modules section.
- Cloud Extender agent v3.000.300.025: Upgrading the core and modules section.

## Cloud Extender 3.000.250 Release Notes

List of features and fixes that are released as a part of Cloud Extender 3.000.250.

Upgrade Signing Certificate.

## Defect Fixes

| Fix # | Description |
|---|---|
| 46320 | Powershell v3 version uses a large amount of space in the `temp` folder. |

For details about all the security issues fixed in this release, see https://www.ibm.com/support/pages/node/7043487

## CVE Security Bulletins

The following CVE security bulletin was issued for this release:

| Affected Product(s) | Version(s) | CVE(s) |
|---|---|---|
| IBM MaaS360 Cloud Extender Agent | 3.000.100.069 and prior | CVE-2023-28322,<br>CVE-2023-28320,<br>CVE-2023-28319,<br>CVE-2023-28321 |
| IBM MaaS360 Configuration Utility | 3.000.210 and prior | CVE-2023-28322,<br>CVE-2023-28320,<br>CVE-2023-28319,<br>CVE-2023-28321 |
| IBM MaaS360 Certificate Integration Module | 3.000.210 and prior | CVE-2023-28322,<br>CVE-2023-28320,<br>CVE-2023-28319,<br>CVE-2023-28321 |
| IBM MaaS360 Cloud Extender Base Module | 3.000.100 and prior | CVE-2023-28322,<br>CVE-2023-28320,<br>CVE-2023-28319,<br>CVE-2023-28321 |
| IBM MaaS360 Exchange ActiveSync Module | N/A | None |
| IBM MaaS360 User Visibility LDAP Module | N/A | None |
| IBM MaaS360 Certificate Integration Module | N/A | None |
| IBM MaaS360 User Authentication Module | N/A | None |
| IBM MaaS360 User Visibility Module | N/A | None |

- Update the IBM MaaS360 Cloud Extender to version 3.000.250.023 or later.
- Apply the IBM MaaS360 Base, Configuration Utility, and Certificates to version 3.000.250 or later.

## Resources

To upgrade Cloud Extender agent v3.000.250.023, see Upgrading the core and modules section.

# Cloud Extender 3.000.200/210 Release Notes

List of features and fixes that are released as a part of Cloud Extender 3.000.200.

For details about all the security issues fixed in this release, see https://www.ibm.com/support/pages/node/7001689 .

## Defect Fixes

| Fix # | Description |
|---|---|
| 45786 | The error message "Maximum limit reached for Hosts not connected" was displayed in the Cloud Extender VPN module Alert History when sending hourly alerts. |
| 45535<br>45457<br>45243 | Email Notifications stopped working after Mail Server migrated clients environment to Modern Authentication. |
| 6883 | Action failure when proxy is configured in Cert Caching feature. |

For details about all the security issues fixed in this release, see https://www.ibm.com/support/pages/node/7042785

## CVE Security Bulletins

The following CVE security bulletin was issued for this release:

| Affected Product(s) | Version(s) | CVE(s) |
|---|---|---|
| IBM MaaS360 VPN Module | 3.000.100 and prior | CVE-2023-2650 |
| IBM MaaS360 Mobile Enterprise Gateway | 3.000.100 and prior | CVE-2023-20863,<br>CVE-2023-26048,<br>CVE-2023-26049 |
| IBM MaaS360 Configuration Utility | N/A | None |
| IBM MaaS360 Cloud Extender Base Module | N/A | None |
| IBM MaaS360 Email Notification Module | N/A | None |

- Apply the IBM MaaS360 VPN Modules to version 3.000.200 or later.
- Update the IBM MaaS360 Mobile Enterprise Gateway(MEG) to version 3.000.200 or later.

## Resources

To upgrade MEG/VPN Modules, see Upgrading the and the modules section.

# Cloud Extender 3.000.100 Release Notes

List of features and fixes that are released as a part of Cloud Extender 3.000.100.

**Distributed Certificate Caching**

The Certificate Integration module supports a cluster mode that allows administrators to group multiple Cloud Extender® Certificate Integration modules into a single group or cluster to enhance the current caching capabilities of Cloud Extender. When an administrator configures a certificate template from the Cloud Extender Configuration Tool that specifies how a certificate is issued to a device, those certificate templates are automatically synchronized between all the Cloud Extender Certificate Integration modules that are members of the cluster, which reduces the load on the Certificate Authority server and prevents the reissuing of certificates if the user switches policies on a device. Administrators no longer need to manually apply certificate templates to each Cloud Extender Certificate Integration module that are members of the cluster. All Cloud Extender Certificate Integration modules in the cluster can also access cached certificates that can be stored on the MaaS360® Portal in an encrypted format, instead of using a shared network drive to access those certificates.

## Defect Fixes

| Fix # | Description |
|---|---|
| 45342 | Cloud Extender 3.x module causes Denial of Service on clients LDAP environment. |

For details about all the security issues fixed in this release, see https://www.ibm.com/support/pages/node/7001689

## CVE Security Bulletins

The following CVE security bulletin was issued for this release:

| Affected Product(s) | Version(s) | CVE(s) |
|---|---|---|
| IBM MaaS360 VPN Module | 2.106.600 and prior | CVE-2022-4450,<br>CVE-2023-0216,<br>CVE-2023-0401,<br>CVE-2022-4203,<br>CVE-2023-0217,<br>CVE-2022-4304,<br>CVE-2023-0215,<br>CVE-2023-0286 |
| IBM MaaS360 Mobile Enterprise Gateway | 2.106.70 and prior | CVE-2022-41915,<br>CVE-2022-41881 |
| IBM MaaS360 Cloud Extender Agent | 2.106.100.008 and prior | CVE-2022-4304,<br>CVE-2023-0215,<br>CVE-2023-0286,<br>CVE-2023-27536,<br>CVE-2023-27533,<br>CVE-2023-27537,<br>CVE-2023-27534,<br>CVE-2023-27538,<br>CVE-2023-27535 |
| IBM MaaS360 Configuration Utility | 3.000.001 and prior | CVE-2022-4304,<br>CVE-2023-0215,<br>CVE-2023-0286,<br>CVE-2023-27536,<br>CVE-2023-27533,<br>CVE-2023-27537,<br>CVE-2023-27534,<br>CVE-2023-27538,<br>CVE-2023-27535 |
| IBM MaaS360 Cloud Extender Base Module | 3.000.001 and prior | CVE-2022-4304,<br>CVE-2023-0215,<br>CVE-2023-0286,<br>CVE-2023-27536,<br>CVE-2023-27533, |

| | | |
|---|---|---|
| | | CVE-2023-27537,<br>CVE-2023-27534,<br>CVE-2023-27538,<br>CVE-2023-27535 |
| IBM MaaS360 PKI Certificate Module | 3.000.001 and prior | CVE-2022-4304,<br>CVE-2023-0215,<br>CVE-2023-0286,<br>CVE-2023-27536,<br>CVE-2023-27533,<br>CVE-2023-27537,<br>CVE-2023-27534,<br>CVE-2023-27538,<br>CVE-2023-27535 |

- Update the IBM MaaS360 Cloud Extender to version 3.000.100.069 or greater.
- Apply the IBM MaaS360 Base, Configuration Utility, PKI Certificates, VPN Modules to version 3.000.100 or greater.
- Update the IBM MaaS360 Mobile Enterprise Gateway(MEG) to version 3.000.100 or greater.

### Resources

To Upgrade Cloud Extender Agent and MEG/VPN Modules:

- MEG/VPN: Upgrading the and the modules
- Cloud Extender agent v3.00.100.069: Upgrading the core and modules

## Cloud Extender 3.00.001 Release Notes

List of features and fixes that are released as a part of Cloud Extender 3.00.001.

Deprecation of Windows 2012 support

Information about upgrading to Cloud Extender 3.x version.

### Defect Fixes

| Fix # | Description |
|---|---|
| 45485 | Identity certificates failure on newly enrolled devices. |
| 45342 | MaaS360 was causing a Denial of Service (DDOS) on the client's LDAP environment. |
| 45317 | Configuring modern authentication for email notifications failure. |
| 44620, 43350 | Certificate Integration module was still displaying in CE after removing the configuration in CE. |
| 43665 | iOS devices were not receiving secure mail notifications. |

# Android Release Notes

MaaS360 Android Release Notes

## Android 8.41/8.40 Release Notes

MaaS360 makes Android app version 8.41/8.40 available on Play Store on 04 January 2024.

**Streamlined contact search with a clearer distinction between Local and Directory contacts >>**

MaaS360 enhances contact search functionality in the MaaS360 for Android app, providing a clearer distinction between local and directory contacts. In the previous releases, all contacts were displayed together and users had to click the Load more link to view contacts from the server.

Now, when users select the new **Search Global Address List** checkbox, MaaS360 retrieves and displays local contacts in the **Local Contacts** section and contacts from the server in the **Directory** section. To initiate a search, users must enter a minimum of four characters. This improvement streamlines contact search and provides a more organized view of available contacts.

**Configure the minimum OS version requirement for Android Enterprise enrollments >>**

MaaS360 now allows administrators to set a minimum OS version requirement for Android Enterprise devices, ensuring that only devices running compatible OS versions are enrolled in MaaS360. When this setting is enabled, only devices running the specified OS version or higher will be able to enroll in MaaS360.

In the past, administrators had to set a minimum and maximum OS version range through Compliance Rules. However, the rule was applied only after a device was already enrolled, leading to delays in unenrolling the non-compliant devices. Users were unsure as to why the devices were unenrolled from MaaS360.

The new feature addresses those issues by validating the OS version up front. Devices that don't meet the minimum OS requirement will be blocked from enrolling in MaaS360, and users will receive a clear error message explaining the reason for the enrollment failure.

The path to the new setting: **Setup** > **Settings** > **Advanced Enrollment Settings** > **Advanced Management for Android Devices** > **Set lowest Android OS version allowed for enrollment**.

**Important information regarding inactive Google accounts and Android Enterprise >>**

Google has recently announced that they reserve the right to delete inactive Google Accounts and their associated data if an account remains inactive for at least two years. This policy applies to personal Google Accounts. Google has clarified that admin accounts associated with Android Enterprise administration are exempt from the inactive Google account policy.

You can follow the recommendations on this page to ensure that your Android Enterprise binding remains active and to avoid disruption to your device management activities.

**Simplified sign-in and sign-out for shared kiosk devices >>**

MaaS360 adds a new policy setting **Show Sign in and Sign Out options for shared devices** to streamline the sign-in and sign-out process for corporate shared devices that are enrolled in Device Owner mode. When this setting is enabled, users can seamlessly sign in and sign out directly in the kiosk launcher. In the previous releases, administrators had to add the MaaS360 app to the app allowlist in COSU policies. This enhancement eliminates the need for users to take the extra step of launching the MaaS360 app simply for authentication purposes.

**Note:**

- Path to the new policy setting: Security > Policies > Android MDM policy > Android Enterprise Settings > COSU (Kiosk mode) > Kiosk Launcher Settings > **Show Sign in and Sign Out options for shared devices**.
- This policy setting is available only in the kiosk multi-app mode. Meaning, that the **Show custom Home page with allowed apps** option should have been selected in the **COSU Mode Type**. This option is not available in single-app mode.

- Other common shared device scenarios, such as policy assignment, app distribution, and app removal, will continue to function as usual.

## Android 8.35 Release Notes

MaaS360 makes the Android app version 8.35 available on the Play Store on 18th October 2023.

**New enhancements to Android Shared device experience >>**

In Android app version 8.30, MaaS360 added improvements to the Shared Device UI, particularly in areas like device enrollment, user sign-in, switching users, and automatic app removal during sign-out. With the Android app version 8.35, MaaS360 continues to enhance the Shared Device UI. The focus remains on creating a better user experience during shared device usage. MaaS360 includes a modern Android design, adds labels to track sign-in and sign-out progress directly on the screen, and enhances error handling for a smoother experience throughout the shared device process.

### Defect Fixes

| | |
|---|---|
| 46620 | Android devices were unable to access Windows File Share through the IBM MaaS360 Mobile Enterprise Gateway (MEG). |
| 46685 | After enrolling devices in the userless mode, users were able to add their personal accounts and access the Play Store on those devices. |

## Android 8.30 Release Notes

MaaS360 makes the Android app version 8.30 available on Play Store on 24th August 2023.

**Enhancements to Android Shared Device experience >>**

MaaS360 adds significant improvements and User Interface changes to enhance the shared device experience for end users. The improvements are primarily focused on areas such as shared device enrollment, user sign-in, switch user functionality, and automatic uninstallation of apps during sign-out.

**Improvements**

- **Reduced Switch User Flow Delays:** The switch user flow has been optimized to significantly reduce delays to approximately 1 minute. In the previous releases, switching between users took up to 3 minutes to sign out of the current user and sign in as the new user.
- **Enhanced user experience**: MaaS360 now shows intermediate stages directly on the screen for users during sign-out, sign-in, and switch user flows. This feature provides real-time feedback and visibility into the progress during each step of the process. For shared device sign-in, MaaS360 shows intermediate stages: Authenticating, Finishing Sign-in, Creating Google user authentication token, Configuring Google Account, Initializing Play apps for user, and Sign-in Complete.
- **Enrollment Failure Messages:** Displays the corresponding enrollment failure messages directly on the screen to help troubleshoot issues encountered during the enrollment process.
- **Enhanced Logging System:** Improved logging to allow administrators to debug issues in the Shared device mode.
- **Resolved G Suite Authentication Issues:** Fixed authentication failures in G Suite accounts during Shared Device enrollment to ensure a smooth and successful enrollment process.
- **Fixed App Installation issue:** Fixed an issue where users were unable to install apps from the Google Play Store. When users tried to install apps, they were redirected to the MaaS360 app from the Google Play Store.

**Granular reporting for Kiosk mode status >>**

MaaS360 introduces granular reporting for Kiosk mode status. The Device Summary page now displays detailed kiosk failure states from both the MaaS360 agent and kiosk apps. The newly added kiosk state labels provide a clear distinction between kiosk failure states (**Error**: Download failed) and kiosk exit states (**Exited**: via Admin action). Administrators can use Advanced Search to filter devices based on these new kiosk states. Additionally, MaaS360 enhances logging to enable administrators to collect detailed failure state information from affected devices. This update addresses multiple defects in devices, where either the Kiosk mode was not applied, or devices exited Kiosk mode upon reboot. Furthermore, MaaS360 evaluates kiosk status during every policy evaluation and attempts to reapply kiosk settings in scenarios where the kiosk exits randomly without a known reason.

Advantages:

- Collects precise failure state information for quicker and more accurate troubleshooting.
- Provides better awareness of the exact kiosk status on devices.
- Saves time in reviewing kiosk-related issues.

**Note:** The device groups created with the old Kiosk mode status in your MaaS360 account are no longer valid. For example, in the new enhancement, MaaS360 has divided the Exited state into granular states. Therefore, administrators must redefine advanced search conditions based on the new Kiosk mode statuses.

**User Interface enhancements in the MaaS360 app >>**

MaaS360 adds new user interface enhancements to streamline the user experience and provide more control over app permissions and settings.

- **Unified Settings UI with single-color icons**: To ensure consistency with the other screens in the MaaS360 app, the settings UI has been redesigned to display all icons in a monochromatic style. Previously, each setting on the Settings screen used different colors.
- **New Required Permissions screen**: MaaS360 adds the new Required Permissions section in the Settings screen to provide visibility into all the permissions required by the MaaS360 app. The Required Permissions screen segregates the permissions into two sections: **Allowed** for permissions that are already granted and **Not Allowed** for permissions that still need to be allowed. When users tap on the permissions listed under **Not Allowed**, they are automatically redirected to the device's settings page where they can grant permission for the MaaS360 app.
- **New Permissions tab in What's New screen**: MaaS360 adds the **New Permissions** tab in the What's New screen to provide visibility into the permissions required for the updated version of the MaaS360 app. This tab displays permissions that are not already granted by users. The required permissions that are already granted to the MaaS360 app are not listed in this section. When users tap on the permissions, they are automatically redirected to the device's settings page where they can grant the permissions.

**Track permissions used by the MaaS360 app in the Privacy Dashboard >>**

When users grant permissions listed in the Required Permissions, they can track how those permissions are used by the MaaS360 app in the Privacy Dashboard. For instance, users can access a timeline detailing when the Location permission was used by the app during the past 24 hours. To view the Location usage timeline, go to device Settings > Privacy Dashboard > Location.

## Android 8.25 Release Notes

MaaS360 makes the Android app version 8.25 available on Play Store on 02 June 2023.

MaaS360 introduces the CDN beta, enabling customers to try out new features on their test devices until the Play Store version of the Android app (version 8.25) becomes available to all customers. The CDN beta offers an opportunity for customers to experience and provide feedback on the new features.

- Enrolling through the QR code: After downloading the QR code from the MaaS360 portal, customers must decode the QR code, replace the agent URL with https://dl.m10.maas360.com/nafo/cdn-content/agents/android/MaaS360AndroidBeta.apk, and then use the newly generated QR code for enrollment.
- Enrolling through KME: Customers must replace the source URL with our Staging link (https://dl.m10.maas360.com/nafo/cdn-content/agents/android/MaaS360AndroidBeta.apk)

- APK: Customers must download the apk from this URL https://dl.m10.maas360.com/nafo/cdn-content/agents/android/MaaS360AndroidBeta.apk and use it for adb installation/upgrade or they can distribute it via App Catalog to update the app on the device.

## New features and improvements

### Android 14 Zero-day support

MaaS360 announces zero-day support for Android 14. With this support, new Android 14 devices enrolled in MaaS360 and existing devices upgraded to Android 14 continue to work seamlessly without disruption. MaaS360 ensures that both IT and end-users can take advantage of the new features that are built into Android's updated operating system from the day of release.

Behavior changes:

When MaaS360 runs on Android 14, there will be behavior changes that impact some of the features in the MaaS360 app.

- Starting from Android OS version 14, MaaS360 no longer supports Device Admin enrollments. If users attempt to enroll Android 14 devices in Device Admin mode, MaaS360 will display an error message and block the enrollment process. However, devices that are already enrolled in Device Admin mode will continue to function properly when they are upgraded to Android 14.

### Fixed device attestation failures

MaaS360 fixes device attestation failures for DO and WPCO enrollments. In the previous releases, the device attestation failed during Device Owner QR code enrollments.

### Improvements in displaying precise IMEI and phone number information in the MaaS360 Portal

MaaS360 incorporates the latest Android APIs to retrieve the IMEI and phone numbers from Android devices. This enhancement ensures that accurate IMEI and phone numbers are now displayed in the Security and Compliance screen in the MaaS360 portal. In earlier releases, MaaS360 used the deprecated Android API, which occasionally resulted in truncated IMEIs being reported. With this update, MaaS360 delivers improved reliability and precise IMEI and phone number information for enhanced device management and security.

### Streamlined enrollment process to install apps on newly enrolled devices without delays

When enrolling a new device, MaaS360 now sets the policy in the background before adding the managed Google Play Account to the device. This change addresses a previous issue where the policy was applied after enrollment, leading to the failure of auto-installing Managed Google Play apps on devices. This enhancement streamlines the device onboarding process and ensures that the desired apps are automatically installed on enrolled devices without any manual intervention.

**Note**: This enhancement does not introduce any behavior or UI changes. The updates are implemented seamlessly in the background, requiring no action from users.

### MaaS360 now uses the latest Apktool for wrapping

MaaS360 uses Apktool, an open-source library tool for Android app wrapping. The MaaS360 portal is now enhanced to use the latest Apktool version 2.70.

The latest version of ApkTool adds the following improvements:

- Support for API 33.
- Enhanced support for AndResGuard / Proguard resource tricks.
- Correct compression handling with remapped resources.
- Enhanced support for applications with multiple styles res types.

### MSAL library upgrade

MaaS360 upgraded MSAL to version 4.4.0. This upgrade does not introduce any changes to the functionality or user interface of the MaaS360 app.

**Note:** MaaS360 plans to upgrade its POI library to 5.2.2 in the upcoming releases. After the upgrade, MaaS360 stops supporting the RMS-protected file or rpmsg file types in PIM and Docs apps on Android 7 and lower devices. The minimum OS requirement for the latest POI library is Android 8 and later.

### Defect Fixes

| Defect # | Summary |
|---|---|
| 46054 | The device attestation failed during Device Owner QR code enrollments. |
| 46159 | Devices stopped reporting phone numbers to the MaaS360 portal. |
| 45590 | Devices requested Wi-Fi certificates multiple times, including inactive devices. |
| 46127 | The Upload logs action status was displayed as **Pending** and the logs were unavailable even after the action was completed. |
| 45767 | Some devices reported truncated IMEI numbers to the MaaS360 portal. |

## Android 8.21 Release Notes

MaaS360 makes the Android app version 8.21 available on Play Store on 17 April 2023.

### Defect Fixes

| Defect | Summary |
|---|---|
| 46054 | Upgraded Play Integrity API to fix intermittent device attestation failures in enrolled devices. |
| 46072 | Users were unable to open the MaaS360 App Catalog in the Kiosk mode. |
| 45959 | Devices did not display time on the status bar in kiosk mode when **Show Custom Status Bar** was enabled. |
| 45913 | Devices had the Secure Browser Gateway enabled despite turning off the Enterprise Gateway in WorkPlace Persona policies and uninstalling the Secure Browser app. |
| 46028 | Activated (non-MDM) devices requested certificates (an MDM action) from the MaaS360 Portal. |
| 46066 | Webapps failed to open on Android 13 devices. |

## Android 8.20 Release Notes

MaaS360 makes the Android app version 8.20 beta available on Play Store on 10 March 2023.

**All MaaS360 apps are now compliant with Android 13 >>**

MaaS360 is now fully compatible with Android 13 and adopts all the behavior changes related to Android 13.

**Notification permission changes in MaaS360 container apps >>**

If a user installs a MaaS360 container app on a device that runs Android 13 or higher, the app's notifications are off by default. MaaS360 displays a new runtime notification permission request on the app's first run. The app notifications wait until the user grants that permission to that app. If users deny the runtime notification permission, MaaS360 displays a rationale screen that explains why the app needs the runtime notification permission, encouraging users to grant the permission.

**Note:**

- The new notification permission request is displayed only on container apps such as MaaS360 core, Secure Browser, Docs, PIM, VPN, Remote Control, and Viewer.
- Notification permission is mandatory for VPN and Remote Control apps.
- The runtime permission request is not displayed if the notification permission was pre-granted to the apps before upgrading to Android 13.

**Support for System Update policies for Work Profile on Corporate Owned (WPCO) devices >>**

MaaS360 extends System Update policies to WPCO devices. Administrators can use these policies to configure when over-the-air system updates are installed on a device. This policy affects the pending system update (if there is one) and any future updates for the device. In the previous releases, these settings were supported only on Device Owner devices.

**Note:**

- If a policy is set on a device, the system doesn't notify the user about updates.
- Supported only on Android 11+ (WPCO) devices.

### Defect Fixes

| Fix # | Description |
|---|---|
| 45896 | Users were not able to view the EULA agreement correctly on Android devices within the MaaS360 app. |
| 45547 | The garbled text was displayed when users opened a corporate website on the Secure Browser app. |
| 45745 | During AE KME Enrollment, if the initial auth attempt failed, MaaS360 did not allow users to navigate to the previous screen to try and authenticate again. |

# iOS Release Notes

MaaS360 iOS Release Notes

## iOS 5.70 Release Notes

MaaS360 makes the iOS app version 5.70 Beta available on TestFlight on 30 January 2024.

Added security fixes and performance improvements.

MaaS360 upgraded the OpenSSL library to 3.0.10 in the following apps:

- iOS Secure Browser 3.93
- iOS Secure Editor 3.40
- MaaS360 PIV-D App 1.60

## iOS 5.61 Release Notes

MaaS360 makes the iOS app version 5.61 available on the App Store on 20th November 2023.

### Defect Fixes

| Defect | Summary |
|---|---|
| 46143 | The iOS Secure Mail app froze when users tried to delete an email. |

## iOS 5.60 Release Notes

MaaS360 makes the iOS app version 5.60 available on the App Store on 06th September 2023.

**iOS 17 zero-day support >>**

MaaS360 announces same-day support for iOS 17. With this support, new iOS 17 devices enroll with MaaS360 and existing devices upgrading to iOS 17 continue to work seamlessly without any disruption.

- **Advanced iOS supervised policy settings >>**

  MaaS360 introduces new supervised policy settings and deprecated some of the existing policy settings for iOS 17 devices.

**Simplified process for adding external documents in the Docs app >>**

The MaaS360 app is updated to eliminate the **Browse** button when adding external documents within the Docs app. When users access the My Docs page, click the + icon, and select the External Document option, MaaS360 will now directly present the device's documents without showing the **Browse** option.

**Redirect users to the support website from the Support screen >>**

Administrators can now get their support website URL embedded on the Support screen in the MaaS360 for iOS app. When users click Contact Support, they are redirected to the support website for contact details. In the previous releases, administrators could display only support email addresses on the Support page. Administrators can directly configure email addresses through the MaaS360 Portal Home page > Setup > Settings > Basic Enrollment Settings > Corporate Support Information.

**Note:** Administrators cannot add the hyperlink through the MaaS360 portal. They need to contact MaaS360 support and provide the URL and link text to get the hyperlink embedded in the Support screen > Support Info section.

### Defect fixes

| Defect | Summary |
|---|---|
| 46229 | Fixed an issue wherein users could not load server emails from the search results in the MaaS360 for iOS app. |
| 46365 | A new certificate was generated by the cloud extender through the auto-renewal process on the renewal date but did not successfully reach the device. Follow these steps to manually renew the certificate on the device:<br>1. Open the MaaS360 Settings app.<br>2. Navigate to **Mail, Contacts, Calendar, Tasks** > **Manage Accounts** > Select the account that you want to renew the certificate for > **Certificate Details** > **Request Certificate**. |

## MaaS360 PIV-D App 1.50 Release Notes

MaaS360 makes the MaaS360 PIV-D app version 1.50 available on Play Store on 23 June 2023.

- MaaS360 upgrades the OpenSSL library in the PIV-D app to version 3.0.8.
- **Discontinued support for iOS 13**

  The MaaS360 PIV-D app version 1.50 is no longer compatible with iOS version 13 and lower. The minimum OS requirement for PIV-D app version 1.50 is now iOS 14. This means that users with iOS versions older than 14 will be unable to download the PIV-D app version 1.50 from the App Store. MaaS360 recommends that customers upgrade to the supported OS versions to take advantage of future MaaS360 app versions.

## iOS 5.50 Release Notes

MaaS360 makes the iOS app version 5.50 available on App Store on 23 June 2023.

### Defect Fixes

| Defect # | Summary |
|---|---|
| 46031 | Some calendar entries were missing in the Secure Mail app.<br>MaaS360 introduced the **Refresh Calendar** option in the MaaS360 app, enabling devices to update missing calendar entries and synchronize meetings with the correct time.<br>**Path**: MaaS360 App Settings > Mail, Contact Calendar, Tasks > Calendar > Refresh Calendar. |

## iOS Secure Browser 3.92 Release Notes

MaaS360 makes the Secure Browser app version 3.92 beta available on App Store on 23 June 2023.

MaaS360 upgraded the OpenSSL library in the Secure Browser app to 3.0.8.

## iOS Secure Editor 3.30 Release Notes

MaaS360 makes the Secure Editor app version 3.30 beta available on App Store on 23 June 2023.

MaaS360 upgraded the OpenSSL library in the Secure Editor app to 3.0.8.

## iOS 5.41 Release Notes

MaaS360 makes the iOS app version 5.41 available on App Store on 24 April 2023.

### Defect Fixes

| Fix # | Summary |
|---|---|
| 46069, 46049 | VPN profiles could not be installed on iOS devices when Endpoint Threat Management was enabled in the MaaS360 Portal. |

## iOS SDK and Wrapping 4.45.000 Release Notes

MaaS360 makes the iOS SDK and Wrapping version 4.45.000 available on 25 April 2023.

### Defect Fixes

| Defect | Summary |
|---|---|
| 45752 | Fixed an issue wherein enterprise apps were unable to connect to MaaS360 Mobile Enterprise Gateway (MEG). |

# macOS Release Notes

MaaS360 macOS Release Notes

## macOS Agent 2.52.000, App Catalog 1.59.100, and App packager 1.49.100 Release Notes

MaaS360 makes macOS Agent version 2.52.000, App Catalog 1.59.100, and App packager 1.49.100 available on October 20, 2023.

**Extended app vulnerability remediation support to macOS >>**

MaaS360 now allows you to remotely remediate app vulnerabilities detected in third-party apps that are installed on macOS devices. Additionally, you can send notifications to users and devices, informing them about app vulnerabilities and the remediation actions.

**OpenSSL library upgrade >>**

MaaS360 upgrades the OpenSSL library in the macOS agent app to 3.0.10.

## macOS Agent 2.50.100 Release Summary

MaaS360 makes macOS Agent version 2.50.100 available on 12 May 2023.

### Defect Fixes

| Defect | Summary |
|---|---|
| 45668 | When administrators submitted shell scrips, macOS devices received and ran those scripts after a delay. |

## macOS Agent 2.50.000, App Catalog 1.59.000, and macOS App Packager 1.49.000

MaaS360 makes macOS Agent 2.50.000, App Catalog 1.59.000, and macOS App Packager 1.49.000 available on 30 March 2023.

### Defect Fixes

| Fix # | Description |
|---|---|
| 45530 | MacOS devices reported inaccurate antivirus and firewall details. |
| 45668 | Shell scripts deployed from the MaaS360 Portal failed to execute on macOS devices. |

## macOS Agent 2.49.000, App Catalog 1.58.000, and macOS App Packager 1.48.000

MaaS360 makes the macOS Agent 2.49.000, App Catalog 1.58.000, and macOS App Packager 1.48.000 available on 24 January 2023.

**New option to install Rosetta in the add enterprise app workflow >>**

MaaS360 adds the new Install Rosetta if required flag in the MaaS360 App Packager for macOS enterprise apps. This option is available only in the new app and upgrade app workflows. Rosetta enables apps built for Macs with Intel processors to run on Macs with Apple Silicon. If this flag is selected, MaaS360 automatically installs Rosetta when the MaaS360 agent installs the macOS enterprise app. MaaS360 ignores this flag if Rosetta is already installed on the device.

IBM®