10.88 Release Summary

Android

New enhancements to Android agent enrollment workflows >>

In Android app version 8.0, MaaS360 revamped Android agent enrollment screens with a new user interface and productivity enhancements. In the previous releases, the new enrollments enhancements were available only to Device Admin bulk enrollments by default. Administrators had to create and embed a custom URL in the HTML file to apply new enrollment changes to Profile Owner, Device Admin, and SPS.

MaaS360 adds the following enhancements in Android app version 8.10:

- Extends new enrollment enhancements to all the enrollment modes (Device Admin, Profile Owner, and Device Owner). All devices automatically go through the new enrollment flow during the enrollment without requiring additional configuration.
- Allows administrators to force the device enrollment as a part of device provisioning so that users cannot skip important device enrollment screens.
- Replaces local authentication screens with a unified webview.
- Removes enrollment completion notification and displays the enrollment status directly on the enrollment screen.
- Displays the number of retry attempts directly on the enrollment screens.

Note: New enrollment screens are available only on devices running Android OS version 7 and later. Requires MaaS360 for Android app version 8.10.

Support to remotely deploy OS upgrade to corporate-owned devices >>

MaaS360 adds a new device-level and group-level dynamic action **Android OTA upgrade** to allow administrators to remotely deploy OS upgrade to Device Owner (DO), WPCO devices, and non-GMS devices. This command uses OS binary package as an input to execute the OS update on devices. Administrators can use device groups to target multiple devices for the OS update. **Prerequisite**: Administrators must get the OS binary package from the corresponding device manufacturer (OEM). For Nexus and Pixel drives, administrators can download the OTA packages from this URL - https://developers.google.com/android/ota

OS requirements:

- Device Owner enrolled devices - Android 10+
- Work Profile on Corporate Owned (WPCO) enrolled devices - Android 11+
- Non-GMS enrolled devices - Android 10+

Android OS versions 5 and 6 is no longer recommended by MaaS360 >>

In Q1 2022, MaaS360 announced the end of support timelines and then constantly reminded customers to target devices running Android OS versions 5 and 6 for OS upgrade or replacement. Effective with MaaS360 agent version 8.10, devices that run these OS versions will no longer receive new MaaS360 apps. The MaaS360 agent app version 8.05 is the last supported version for devices running OS versions 5 and 6. If there are issues or bugs with OS versions 5 and 6, customers cannot raise support tickets for problems that occur on these OS versions.

Customer impact on devices running OS versions 5 and 6:

- Devices that are currently enrolled can continue to be enrolled and secured until further notification. These devices are automatically locked to the MaaS360 app version 8.05.
- New devices can be enrolled with MaaS360 app version 8.05, which is the last supported agent version on unsupported devices.
- Effective with MaaS360 SDK version 8.10, MaaS360 freezes support for these older versions. The minimum OS version requirement for the MaaS360 SDK jar 8.10 is Android 7 and later.
- The apps that are wrapped or updated after the 10.88 release are compatible only on Android devices running OS versions 7 and later. Existing apps continue to work on older OS versions unless they are updated or re-wrapped after the 10.88 release. If customers want to manage both existing and new apps, the apps wrapped after 10.88 release must be added as an additional version.

End of support announcement for Knox enrollments on Android OS version 7 >>

Samsung announced the end of support for Knox enrollments on Android OS version 7 in the policy update statement. As per the policy update, Samsung updated the minimum supported versions to restrict Knox enrollments to Android OS versions Android 8.0 (Knox 3.0) and later. For more information on the policy update, see https://www.samsungknox.com/en/blog/policy-update-on-knox-supported-versions.

To comply with Samsung's policy update requirements, MaaS360 no longer supports Samsung Knox enrollments (new/re-enrollment) on Android OS version 7 effective with MaaS360 for Android app version 8.10.

Impact:

- Existing devices - Android 7 devices that are already enrolled into MaaS360 are unaffected, but they will not be able to re-enroll.

- New devices - Android 7 devices can no longer enroll with MaaS360 for Android app version 8.10.

Updated messaging in the MaaS360 for Android app to improve end-user transparency >>

MaaS360 improves messaging in some permission request and dialog boxes that are presented in the MaaS360 for Android app based on Google's privacy policies.

MaaS360 adds the following enhancements:

- Updated permission dialogs based on Google's best practices to make permissions more understandable, useful, and secure for users. The updated permission dialogs clearly explain what data the MaaS360 app is trying to access and what benefits the app can provide to the users if they grant that permission. In scenarios where the permission is critical to the functioning of the MaaS360 app, MaaS360 displays a rationale screen to explain why the permission is required and what functionalities are affected if the permission is denied.
- When users try to remove MDM control, MaaS360 presents an additional dialog that clearly explains the functionality impact so that users can take informed decisions.
- Displays the list of all the policies that are enforced by the organization to manage devices.

Support to configure custom policy restrictions on managed devices >>

MaaS360 now allows administrators to create custom policy restrictions that aren't built in to the MaaS360 portal. The custom policies include the features and settings that administrators can control on managed Android Enterprise devices.

Configure time for the kiosk device to return to the single app mode >>

MaaS360 adds a new policy setting to allow administrators to configure the time before the configured app is automatically launched when users exit the single app mode. Users exit the single app mode to perform activities such as changing device settings and checking the billing ID. In the previous releases, the timer was automatically set to 60 seconds by default. If this setting is not configured, the configured app is automatically launched 60 seconds after users exit the single app mode.

Note: Supported only for the single app mode. COSU Mode Type must be set to **Automatically launch a required app and lock the device to display only this**.

Path: **Android Enterprise settings** > **COSU (Kiosk mode)** > **Time after which app should be launched automatically (in seconds)**.

iOS

New device summary parameter to track when the MDM command was last executed on the device >>

MaaS360 adds a new device summary parameter **MDM Last Reported Time** under the WorkPlace & Security section. This parameter displays the time the native MDM client on the device reached the MaaS360 Portal to pick any waiting commands such as lock device, change policy, and wipe device.

Note: The **MDM Last Reported Time** parameter should not be confused with the **Last Reported** parameter, which displays the time the MaaS360 agent or MDM client last reported to the MDM Portal.

Fixed an issue with a push iOS update command and other usability improvements >>

MaaS360 fixed an issue where the push OS update command **Download and Install** could not execute the installation after downloading the software update. Effective with 10.88, when administrators issue the **Download and Install** command, MaaS360 downloads the software update and then automatically installs the previously downloaded software update. In the previous releases, administrators had to issue the Download and Install command twice. There is no impact to the other push iOS update commands: **Download only** and **Install earlier downloaded updates immediately**.

MaaS360 removes the **Distribute updates over** option in the Push iOS Update group-level action. As a result, the iOS update command is executed immediately without a delay. In the previous releases, administrators could distribute OS updates over a period of time to avoid network congestion.

Platform

Enhancements to License Management Alerts >>

The license expiration alert sent to administrators when a license is about to expire has been enhanced as follows:

- For trial customer accounts, an email notification is sent to the customer 15 days before the trial subscription expires.
- The email notification is not sent to customers who opted for auto-renewal of the license subscription.

Support device enrollment for suspended license bundles >>

MaaS360 allows enrollment of new devices to suspended license bundles for a configured period. This feature is useful in cases where a customer raises renewal request for a license subscription and the renewal process takes some time. This enhancement helps the customer to receive uninterrupted service and add new devices to the suspended license bundles for the configured temporary period until the subscription turns active.

Previously, a suspended license bundle could not be assigned to new devices, and this caused disruption in the services offered to customers during this period.

If you have raised renewal request for a suspended license bundle, contact MaaS360 Support to get this feature enabled for your account until your request is successfully processed and the subscription becomes active.

Support revocation of licenses from a device in the Inactive or Pending Remove Control state >>

In the previous releases, the licenses assigned to a device remained assigned even if the device moved to an inactive state. Administrators could not revoke the license from an inactive device if the device did not return to an active state. As a result, the License Overview page displayed incorrect count for the total license units consumed.

Effective 10.88, Administrators can revoke the license entitlements that are assigned to a device that is in an Inactive or Pending Remove Control status. As a result, the License Overview page displays correct count for the total license units consumed.

Enhancements to the Auto App Addition Status for the VPP Token upload >>

MaaS360 enhances the UI of the Token Details page for improved usability. The changes include the following:

- A column name is modified.
- The Comments column displays additional information on the Auto App Addition Status of the apps that are automatically added to the App Catalog from the VPP Token upload.

Enhancements to the administrator details >>

The administrator details displayed on the Administrators page have been enhanced as follows:

- Includes date and time of the last successful login of an administrator into the MaaS360 Portal.
- Excludes the Authentication Status of the administrator who logged in to the MaaS360 Portal.

Track policy distribution progress for iOS devices >>

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

Security Dashboard enhancements >>

MaaS360 adds usability improvements and significant security enhancements in the Security Dashboard. The widgets in the Security Dashboard are consolidated and arranged in a single layout so that the important information is immediately accessible at a glance. The detailed information about the affected devices in the Top risk incidents widget is displayed on new pages instead of a modal window.

MaaS360 adds the new Security Events widget in the Security Dashboard. This widget displays an aggregate view of all security events that were detected in the past 60 days. The security events are categorized based on whether a risk rule is configured for those events. MaaS360 uses separate color codes to clearly differentiate the events that have risk rules configured from the events that do not have risk rules configured in the MaaS360 Portal. Administrators can drill down to the Security Events page from this widget, where they can view the detailed summary of exposed devices, track the event types without risk rules, and enhance security by modifying the risk rules or configuring new risk rules. Administrators can also track the top 5 event types without risk rules that contributed to the most security events in their organization. For more information on Security Events widget, see https://www.ibm.com/docs/en/maas360?topic=devices-security-dashboard-widget-security-events.

These enhancements allow administrators to identify security vulnerabilities in their organization and help them make informed decisions such as configuring risk rules and updating policy settings.

Web services API

The following API was updated for this release:

- Search Action History (v1): A new sample response attribute named *result* was added to the API that fetches a detailed description about the status of the actions that were taken on a device.

What's New Since 10.87 Release Summary

Version 10.87.cd.12102022 Released 12 October 2022

Policy modernization support for iOS policies >>

In the previous releases, MaaS360 added policy modernization framework for Android and Windows platforms. In this release, MaaS360 extends the policy modernization enhancements to the iOS platform. In the redesigned framework, MaaS360 simplifies user experience, improves performance, and adds significant enhancements to policy configuration, policy assignment, review changes, policy audit, and bulk update workflows.

Highlights

- Flagging invalid policy configurations with an error icon.
- Review policy parameter changes at the policy setting level with the help of color codes.
- Real-time validation of policy configuration.
- New search widget support for all policy settings.
- New filter to narrow down iOS policy settings.
- Simplified bulk update flow.
- Support to track policy change history for more events.
- Support to track all policy assignments in one place.

Availability of modernized security policy workflows:

- For existing customers, modernized security policy workflows will be available in a phased rollout.
- For new customers, modernized security policy workflows are available by default.

Version 10.87.cd.28092022 Released 28 September 2022

Enhancements to Threat Management and Security Dashboard >>

IBM MaaS360 modernizes existing Threat Management and Security Dashboard workflows by adding new detection capabilities, and responses in addition to near-real-time processing of threat incidents, and a new security centric policy. For more information on MaaS360 Endpoint Threat Management, see https://www.ibm.com/docs/en/maas360?topic=maas360-endpoint-threat-management.

Version 10.87.cd.06092022 Released 06 September 2022

Enhancements to the Policy Precedence UI >>

MaaS360 revamps the Policy Precedence UI with an intuitive design and modern user interface. In the redesigned framework, administrators can easily provide policy precedence value or use + and - icons to adjust the precedence instead of drag and drop. MaaS360 also makes it easier for administrators to narrow the list of policies, change policy precedence, and track the impact of policy change on existing devices and groups.

10.87 Release Summary

Android

Knox E-FOTA on MDM to be deprecated 31 July 2022 >>

Knox E-FOTA on MDM is an enterprise solution that allows remote management of Samsung firmware updates for managed devices through MDM solutions. Samsung announced the end of service for Knox E-FOTA on MDM in favor of its successor Knox E-FOTA One. MaaS360 removes the Knox E-FOTA on MDM integration from MaaS360 portal in July 2022. Managing Knox E-FOTA firmware updates in the MaaS360 portal is no longer possible after 31 July 2022. However, customers can continue to deactivate licenses through the MaaS360 portal after 31 July 2022.

Deprecation of app approval in managed Google Play and its impact on MaaS360 app management >>

Google announced deprecation of app approval in managed Google Play. To align with Google's strategy, MaaS360 disables app approval in the MaaS360 portal effective 10.87 release. This deprecation will impact app management workflows in MaaS360 that currently use app approval APIs.

Android 13 Zero-day support

MaaS360 announces zero-day support for Android 13. With this support, new Android 13 devices enroll with MaaS360, and existing devices upgrading to Android 13 continue to work seamlessly without any disruption. MaaS360 ensures that both IT and end-users take advantage of new features built into Android's updated OS from the day of release.

- **Notification runtime permission >>**

  Android 13 introduces a new runtime notification permission, allowing users to focus on the notifications that are most important to them. The notification permission is turned off by default on Android 13 devices. Apps that are installed on Android 13 devices (or devices that upgraded to Android 13) will now request the notification permission before posting notifications. Users must explicitly grant the permission for the notifications to work. For Android Enterprise devices, MaaS360 automatically grants notification permission to core app, PIM, Docs, Browser, VPN, and Remote control. Administrators can use Android Enterprise policies to remotely control notification permission on the managed apps, and also to block apps that use the notification permission on managed devices. For device admin and SPS activated devices, users must explicitly grant notification permission for MaaS360 first-party apps from the corresponding app.

End of Life for Kiosk Mode on Standard Device Admin Devices >>

Google deprecated legacy Device Admin for enterprise use effective with the Android 10 Q release. As a part of this deprecation, a number of Device Admin APIs are removed from support over time. To promote the adoption of Android Enterprise mode, MaaS360 stops supporting Kiosk mode on standard (non-OEM) Android 13 devices that are enrolled in the Device Admin mode.

Note:

- There is no impact to Android devices running OS version 12 or lower. Customers can continue to use Kiosk mode on Android 12 and lower devices without any disruption.
- This deprecation does not impact supported OEM devices. Customers can continue to use Kiosk mode on Samsung, LG, Bluebird, and Zebra.
- There is no impact to Android devices that are enrolled in the Android Enterprise mode.
- Requires MaaS360 for Android app version 7.95+.

Impact on Android 13 Device Admin devices:

- Kiosk policies are no longer supported on standard Android 13 devices (with an exception for OEM devices such as Samsung, LG, Bluebird, and Zebra).
- The options to launch Kiosk mode are unavailable for users when they upgrade to Android 13.

Platform

Revamped Policy workflows for intuitive design, faster performance, and advanced features >>

MaaS360 modernizes security policy workflows with fresh looks and intuitive design. The redesigned interface simplifies the user experience, optimizes performance, and introduces new productivity enhancements.

In the redesigned framework, MaaS360 adds significant enhancements to policy configuration, policy assignment, review changes, policy audit, and bulk update.

Highlights

- Flagging invalid policy configurations with an error icon.
- Review policy parameter changes at the policy setting level with the help of color codes.
- Real-time validation of policy configuration.
- New search widget support for all policy settings.
- Simplified bulk update flow.
- Support to track policy change history for more events.
- Support to track all policy assignments in one place.

Note: These enhancements are rolled out to all customers by default. For existing customers, MaaS360 migrates policy settings and corresponding values to the new framework.

Enhancements to Administrator Audit Reports for Administrator Role Changes >>

The Administrator Audit report generated for the administrator role changes has been enhanced for improved usability. The report is modified to delete unused column data, and logically group data for easier comparison. This is helpful to review the data for auditing purposes.

Note:

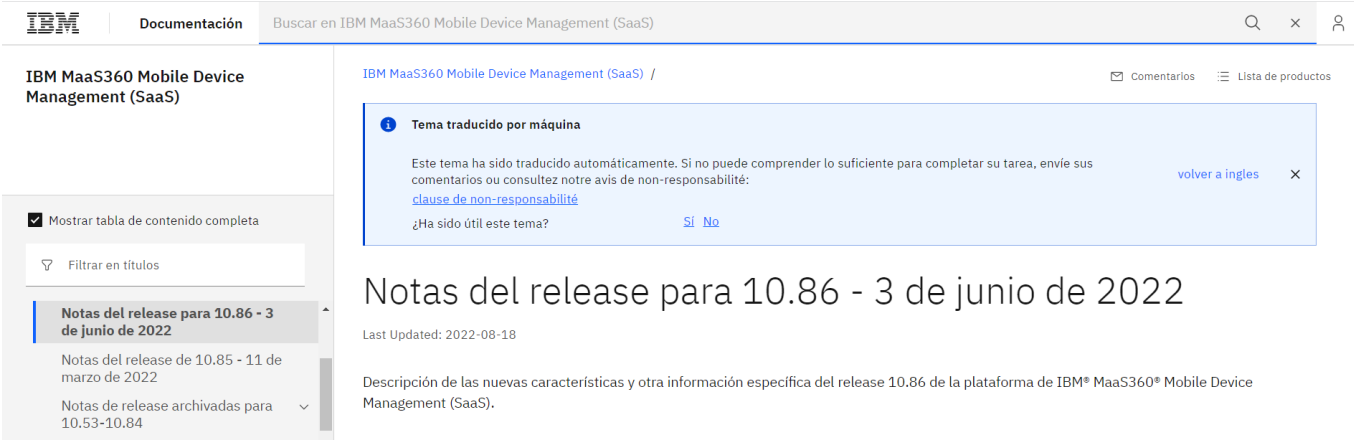
- This feature is not available to all customers by default. Contact MaaS360 Support to get this feature enabled for your account.
- The Role change history report provides the role change history details for a selected administrator account for the previous 180 days. For more information, see https://www.ibm.com/docs/en/maas360?topic=maas360-portal-administration-audit-reports.

MaaS360 IBM Docs site content is now automatically translated to 12 languages >>

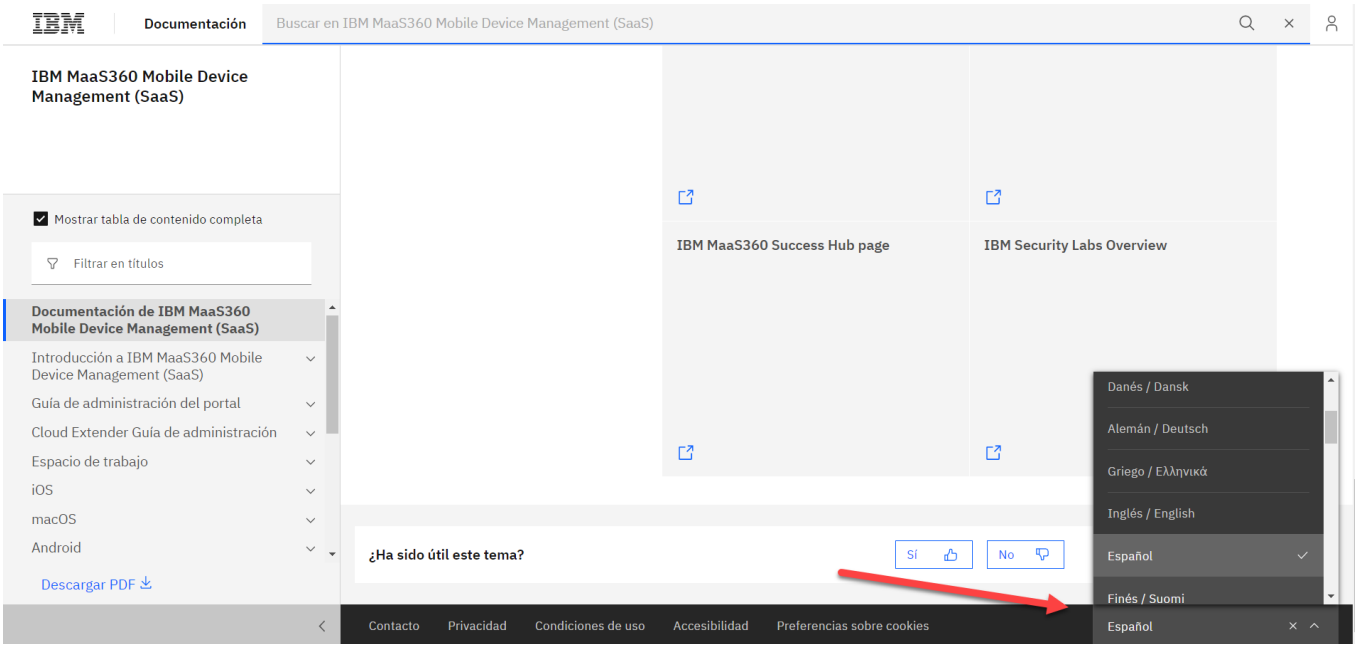
The MaaS360 content that is published on the IBM Docs site is now automatically machine-translated in near real-time using IBM Watson Translation Services for the following 12 languages:

- Brazilian Portuguese (pt-br)
- Czech (cs)
- French (fr)
- German (de)
- Italian (it)
- Japanese (ja)
- Korean (ko)
- Polish (pl)
- Simplified Chinese (zh-tw)
- Spanish (es)
- Traditional Chinese (zh-ch)
- Turkish (tr)

Machine-translated pages: Any content that is machine-translated displays a banner and a disclaimer stating that the content has been machine-translated and provides users the option to revert back to English and to submit feedback:



Switching from English to a machine-translated language: Scroll to the bottom of the IBM Docs site window and click on the language that you want to view (to switch back to English, click on English):



macOS

Deprecation of System Preferences policy settings on macOS 13 >>

Apple deprecated managed System Preference profile, the payload that configures the preference panes on managed macOS devices. There is no impact to versions below macOS 13. Administrators can continue to configure this restriction on devices that run macOS 10.7–12.0.

Support for advanced policy restrictions for macOS 13+ devices >>

MaaS360 adds new policy restrictions: **Allow Universal Control** and **Allow UI Configuration Profile Installation,** allowing administrators to remotely control device restrictions on managed devices.

- **Allow Universal Control** - If set to false, disables Universal Control.
- **Allow UI Configuration Profile Installation** - If set to false, prohibits the user from installing configuration profiles and certificates interactively.

Path: macOS MDM policies > Restrictions > Functionality.

Moved GlobalHTTPProxy payload to device context >>

MaaS360 moves the GlobalHTTPProxy payload from user context to device context.

Changes to the deployment of Policy Preferences Policy Control (PPPC) profile >>

If Global proxy settings are configured through policies, MaaS360 now automatically deploys PPPC profiles during the device enrollment.

Cloud Extender/Mobile Enterprise Gateway (MEG)

New health check alerts for MEG for Apple WKWebview >>

New Enterprise VPN Gateway alerts evaluate the status of MEG and, if triggered, notify administrators by email message or text message about the following events:

- Relay server is not reachable
- DNS settings are invalid or corrupted
- Maximum limit reached for hosts that are not connected

From the MaaS360 Portal, administrators can choose remediation actions to troubleshoot the events.

New TCP settings for MEG in the Cloud Extender Device view on the MaaS360 Portal >>

TCP settings were added to the Cloud Extender Device view to assist administrators with troubleshooting issues with MEG.

Webservices

No APIs were added or updated for this release.

What's New Since 10.86 Release Summary

Version 10.86.cd.15062022 Released 15 June 2022

Enhancements to the exported security policy report >>

You can export policy configurations in the form of an Excel spreadsheet. The export data has been enhanced to introduce new columns to display required information and logically group the data for improved usability. This is helpful to review the data for auditing purposes. For more information on exporting a security policy, see https://www.ibm.com/docs/en/maas360?topic=policies-exporting-security-in-maas360.

Note: This feature is available to customers who have migrated to the new Policy UI. This feature will be rolled out to all customers in phases.

10.86 Release Summary

Android

Configure background apps for Android Kiosk mode >>

MaaS360 now allows administrators to configure background apps on devices that are locked to single app or multi-app kiosk mode. Background apps are hidden from the kiosk launcher and users cannot interact with them. Kiosk apps invoke these background apps to execute essential system functions. For example, you can add Android System Web View (`com.google.android.webview`) as a background app to render web content on some Android devices. **Note**: Supported only for Android Enterprise devices.

Control notification permission for managed apps through Security policies >>

Android 13 introduces a new runtime notification permission, allowing users to focus on the notifications that are most important to them. Apps that are installed on Android 13 will now request the notification permission from the user before posting notifications. Effective 10.86, MaaS360 makes it easier for administrators to control notification permission through Security policies. Administrators can use Android Enterprise policies to automatically grant notification permission to the managed Google Play apps, and also to block apps that use the notification permission on managed devices. **Note**: Supported only for Android Enterprise devices.

Deprecation of app approval in managed Google Play and its impact on MaaS360 app management >>

Google announced deprecation of app approval in managed Google Play. To align with Google's strategy, MaaS360 will disable app approval in the MaaS360 portal effective 10.87 release. This deprecation will impact app management workflows in MaaS360 that are currently use app approval APIs.

Google Play app management enhancements >>

- **Granular instant installation options** - MaaS360 adds new granular instant installation options for Google Play apps - Install once and Retry installation. These options are available in the Add app workflow and the App Summary page. Instant once is the default option for the existing apps that have the Instant Installation option selected. Both the options install the app on devices automatically.
- **New granular installation state for the Install once option** - When an app is distributed with the Install once option, the Status is changed to **Distributed** and State is changed to **App Available with auto install once setting** in the App Distribution page.
- **Support for asynchronous API for better management of apps** - In the previous releases, MaaS360 used different synchronous APIs for various app management tasks, which caused issues in app config distribution and app distribution. Effective 10.86, MaaS360 moves to the newer Google API (asynchronous), wherein all those tasks are performed by a single API and thereby reducing the delays occurring across app config and app distributions.
- **Removed deep link support for app installation** - Users can no longer use deep links to install apps directly from the Play Store.

Use package name to configure an Always On VPN profile through Security policies >>

In the previous releases, MaaS360 supported only a limited pre-defined set of VPN connection types: F5 Edge Client, Pulse Secure, MaaS360 VPN, Cisco AnyConnect, and Aruba VIA. MaaS360 now allows administrators to use the package name (Application ID) of the target VPN application to configure an Always On VPN profile.

Path: Security > Policies > Android Enterprise policies > VPN > Enable Always on VPN > Always on VPN Package Name.

Note:

- Requires MaaS360 for Android app version 7.85+
- This configuration is applied only if a VPN Type is not selected. If you provide both VPN type and Always on Package Name, then VPN type is applied on the device.

iOS

Support for passcode-based DEP enrollments for managed devices >>

- The Basic Enrollment Settings have been enhanced to support passcode-based DEP enrollment for managed devices**. Note:** The administrators who use the passcode-based DEP enrollment for managed devices have an action item and must ensure to manually disable this setting within the specified time. For more information, see https://www.ibm.com/docs/en/maas360?topic=portal-configuring-directory-enrollment-settings-in-maas360.
- While adding devices to send enrollment request, the Override authentication mode for enrollment with passcode option is deprecated for enrolling DEP devices. For more information, see https://www.ibm.com/docs/en/maas360?topic=portal-adding-devices-in-maas360.

Windows

Multiple application support for Kiosk mode (assigned access) apps (UWP and Win32) >>

MaaS360 now supports multi-app kiosk mode for UWP (Universal Windows Platform) and Win32 (Windows desktop applications) on Windows devices. With Kiosk mode (assigned access), administrators provide limited access to an end-user device by restricting access to a few apps. End users can only access apps that are in kiosk mode after signing in to the device.

With multi-app support, administrators can configure up to 10 apps in a single group in kiosk mode on end-user devices by enabling the **Multi app Kiosk (recommended)** option in the updated Kiosk Mode (Assigned Access) policy (**Security > Policies > Windows MDM policy > Advanced Settings**). Administrators can also apply the same kiosk profile to multiple users on the device. The new kiosk apps are displayed on end-user devices in a standard 2x2 tile size and will be available for all configured users.

In previous releases, administrators could only create a single app in kiosk mode for UWP apps only. Multi-app configurations were not supported.

Platform

Creating an app configuration using an existing configuration >>

Administrators can now use an existing app configuration as a base for creating a new app configuration. In the previous releases, administrators had to build new configurations from scratch. When adding a new app configuration, administrators can toggle the **Create from existing configuration** option to select from the list of existing app configurations. **Note**: Supported for both Android OEM/App configuration and iOS App configurations.

Enhancements to license management

- MaaS360 provides the following administrator settings which can be configured to send alert notification emails to the customer:
  - License Usage Threshold: Sends an email notification to the user when the usage of a MaaS360 service license bundle (MaaS360 Part Name) exceeds the configured threshold.
  - License Exhaustion: Sends an email notification to the user when a MaaS360 service license bundle (MaaS360 Part Name) is completely utilized.

  For more information on this enhancement, see https://www.ibm.com/docs/en/maas360?topic=portal-configuring-administrator-settings-in-maas360.
- MaaS360 provisions the following email notifications to the user:
  - When a license assignment request is submitted to MaaS360, an acknowledgment email for request submission is sent to the user who submitted the request. This email includes an attachment with the details of the selected licenses.
  - After successful completion of license assignment, a process completion mail is sent to the user who submitted the request. This email includes an attachment with details of successful and unsuccessful (if any) license assignments.
  - If the license assignment fails due to any technical issue, a process failure mail is sent to the user who submitted the request

  For more information on this enhancement, see https://www.ibm.com/docs/en/maas360?topic=management-license-overview.

Enhancements to Administrator Audit reports

- MaaS360 now records the Delete action in the Administrator Audit > Administrator Changes report. This feature makes it easier for administrators to track administrator account deletions in the MaaS360 portal. The administrator audit report now records details of the delete action such as time of deletion, admin who performed the action, etc. In the previous releases, the report included the details about all the actions performed on the administrator accounts except the delete operation. For more information, see https://www.ibm.com/support/pages/node/6590847.
  Note:
  - The username, email, and other details of the deleted user are masked in the report.
  - This feature is not generally available. Contact MaaS360 Support to get this feature enabled for your account.
- The Administrator change history report provides the change history details for a selected administrator account for the previous 180 days. For more information, see https://www.ibm.com/docs/en/maas360?topic=maas360-portal-administration-audit-reports.

App Management

Support for disabling app reviews on the MaaS360 Portal and end-user devices >>

The App Settings have been enhanced with a new setting to perform the following:

- Disable the Reviews section in the end-user app catalog for iOS and Android devices for a customer. The user is not allowed to provide or view the reviews given for an app.
- Disable the Reviews from users section in the App Catalog on the Portal. The reviews given for an app are not visible to the Administrator.
- Hide the Enterprise App Rating in the App Catalog on the Portal. The rating given for an app is not visible.

Support for bulk deletion for app and bundle distributions >>

MaaS360 supports the selection of multiple app and bundle distribution records to perform bulk deletion. For more information on this enhancement, see https://www.ibm.com/docs/en/maas360?topic=catalog-tracking-app-distributions and https://www.ibm.com/docs/en/maas360?topic=bundle-tracking-distributions.

Deprecation Notice

MaaS360 Multi Policy Feature Deprecation>>

Multi policy feature allows administrators to assign multiple policies to devices. MaaS360 has removed the multi policy feature from all MaaS360 environments in this release.

Webservices

The following web services were added or updated for this release:

- The Get Admin Changes Audit API has been enhanced to fetch audits with the Deleted account status.
- The Add Local User Account API has been enhanced to include a new parameter *emailSetPwdLink* that sends an email link to the user to set a password.

For more information, see the latest Webservices guide.

10.85 Release Summary

Android

New permission dialog for requesting location accuracy on Android 12 devices >>

On Android 12 or higher, users can specify the accuracy of the locations they share by choosing between Precise (`ACCESS_FINE_LOCATION`) or Approximate (`ACCESS_COARSE_LOCATION`) location accuracy.

When the MaaS360 app targets Android 12, the new system permissions dialog includes the following options for the user:

- **Precise**: Allows the MaaS360 app to get precise location information.
- **Approximate**: Allows the MaaS360 app to get only approximate location information.

The Precise location pinpoints the device's location down to a few meters. MaaS360 uses this level of location accuracy to perform some of the crucial functions such as enabling geo-fencing, detecting insecure Wi-Fi connections, and recognizing the device's entry into preconfigured locations. MaaS360 Kiosk app requires this permission to display configured Wi-Fi networks and Bluetooth devices in close range.

Automatic generation of consistent device ID for Android 11 and lower devices >>

Google generates an enrollment-specific identifier for the device as a part of Android Enterprise enrollment. This identifier remains consistent even if the work profile is removed and enrolled again (to the same organization), or the device is factory reset and re-enrolled. To avoid a trial of duplicate device records, MaaS360 uses the same identifier for the device re-enrollment. In the previous releases, administrators had to enable this feature for Android 11 or lower devices through device enrollment settings. In this release, MaaS360 removes the parity between Android 11 and 12 versions and automatically enables this capability for all Android Enterprise devices.

Platform

Enhancements to Settings in the MaaS360 Portal >>

- The MaaS360 Portal UI has been enhanced to replace the term Local with MaaS360 Directory.
- The User Password settings have been enhanced with the following changes:
  - Administrators have the provision to auto-generate or manually set a password or disable password generation for users during account creation in MaaS360 (Local) Directory.
  - The options to generate a password on request from an administrator or during App Catalog distribution and to automatically generate a user password during new device enrollment have been deprecated.
- The customers with Unified Sign-in enabled can disable the MaaS360 (Local) Directory user authentication type to restrict authentication for users belonging to this type.

Support self-serviceable onboarding for existing customers to device-based license management >>

MaaS360 provisions self-serviceable onboarding for existing customers to enable device-based license management for themselves. When a customer enables license management, MaaS360 generates a license assignment report based on the current usage of the services by the existing devices which the customers can confirm to migrate their existing devices to license management.
Note: This feature is not generally available and will be rolled out to eligible customers in phases.

The custom user attributes value for the text attribute is increased from 10 to 15 >>

Administrators can now define a maximum of 30 custom user attributes which includes 15 text or string attributes, two secure value attributes, and five attributes each of date, enum, or boolean.

Per app VPN changes >>

If the policy contains multiple per app VPN profiles (for example Cisco and F5), the payload does not install on ios 15 devices.

Action - Administrators must publish the policy containing multiple per app VPN profiles to allow MaaS360 to push and reload the VPN payload on iOS devices.

Note: The policies that have a single per app VPN profile (for example only Cisco) do not have an impact.

Deprecation notice

MaaS360 Multi Policy Feature Deprecation >>

Multi policy feature allows administrators to assign multiple policies to devices. In the upcoming Q2 2022 10.86 MaaS360 release, MaaS360 will remove the multi policy feature from all MaaS360 environments.

Windows

New Windows 11 Readiness report>>

MaaS360 introduces a Windows 11 Readiness report that uses real-time data to show the Windows devices on your network that are ready to upgrade to Windows 11.

The report provides two dashboards: Summary and Readiness Criteria.

- The Summary dashboard shows the overall readiness of Windows devices on your network to upgrade to Windows 11. You can filter data for devices as ready, not ready, or not available.
- The Readiness Criteria dashboard shows which devices are ready to upgrade to Windows 11 based on whether the device meets the minimum requirements from Microsoft for the following criteria: TPM, storage, memory, system firmware, processor speed, and display. For more information about upgrading your devices to Windows 11, see https://support.microsoft.com/en-us/windows/getting-ready-for-the-windows-11-upgrade-eb50813f-c7da-4cf8-89a3-6ba0d33b2773.

Users can export data from the report to a CVS file and send the report to recipients who are signed up to receive the report.

Webservices

The following new API was added for this release:

- The Get Audit of Ruleset Changes API fetches audits of all rule changes that were made within a specific timeframe for the billing ID of an organization.

Cloud Fixes Summaries

MaaS360 Cloud Fixes Summaries

November 2022 Daily Fixes Summary

MaaS360 Daily Fixes - November 2022

Fix	Description	Release Date
45485	Newly enrolled devices did not receive certificate-based profiles.	01-Nov-22
44958	The Forgot Pin screen in the Android agent app displayed an error message after authentication.	03-Nov-22
45051	Administrators were unable to update certificates on iOS devices through the Update Device Certificate action.	04-Nov-22
45278	The sim card removal notifications were issued with a delay.	04-Nov-22
45496	The option to select Modern Auth was unavailable in App Config for the Outlook app.	07-Nov-22
43137	Automatic deletion of inactive users and devices after 90 days failed.	08-Nov-22
45367	MaaS360 displayed an incorrect Source IP Address in the View Change History.	09-Nov-22
45139	The deleted administrators continued to receive email notifications from the MaaS360 portal.	09-Nov-22
45451	After the MDM control was removed, a blank page was displayed when administrators tried to open the device summary page. As a result, administrators could not issue the Hide device action to the device.	09-Nov-22
44996	When customers enabled Azure AD SAML SSO auth for portal admin login, the redirect URL for the web session failed to load.	09-Nov-22
45261	MaaS360 reports were sent sporadically even though customers activated daily subscriptions.	10-Nov-22
45365	MaaS360 Portal displayed an incorrect number of licenses available for the account.	10-Nov-22
45519	iPadOS devices were unable to access the enrollment URL when they use the mobile desktop view.	10-Nov-22
45410	Endpoint Security policies were unavailable in the MaaS360 portal.	11-Nov-22
45395	Azure AD child groups are not synced to the MaaS360 Portal.	17-Nov-22
45476	The location name was not displayed in the Device history under the Comments when the policy is changed due to location changes.	18-Nov-22

10.88 Release Fix Summary

The following customer issues were fixed in the 10.88 release:

Fix number	Description
43137	System was failing to delete user records after 90 days.
43288	iOS update pushing to devices failed from the Portal.
44052	No filter options available on the PC Inventory Software report after subscribing for email delivery.
44500	Unable to upload Android Enterprise on the MaaS360 Portal.
44897	Enrolling devices failed after account expired and was converted to a trial account.
45072	Old VPN configuration was being applied to devices.
45215	Partner was unable to view their account page (page kept loading).
45599	Unable to log in to the Portal with AD credentials.
44026	Addressed pen testing findings.
44195	iOS policy settings were missing under Supervised Settings.
45007	Admin attempted to add a default domain.
45119	Missing password field in the CardDav iOS policy.
45120	Admin security check for portal actions failed to authenticate.
45123	IBM Verify customer incorrectly listed as trial.
45161	Long URL custom attribute error.
45244	Initial SSO setup wasn't working.
45345	Android Chrome Managed App Config was not working as expected.
45394	Discrepancy with the count number for all administrators.
45469	App Client ID information on Admin Portal was updated.
45509	Email field was not being saved in the Maas360 Portal compliance rules for the Standard Email List.
45514	License overview count was displaying more units consumed than what was displayed on the main dashboard page.
44469	Advanced Search Criteria "Configurator Supervised Mode" out of alphabetical order and was possibly mis-labeled.
45301	API call updated for Stop Distribution API.

October 2022 Daily Fixes Summary

MaaS360 Daily Fixes - October 2022

Fix	Description	Release Date
45225	Administrators could not initiate remote control using the Remote Support app on Samsung SM-A336E models.	11-Oct-22
45312	The App Allowlist in iOS Supervised Settings did not return matching results against the search input provided by the administrators.	12-Oct-22
45383	Administrator Log in reports displayed an incorrect IP address.	13-Oct-22
45404	The apps in the App Catalog were not updated automatically.	14-Oct-22
45395	Azure AD child groups are not synced to the MaaS360 Portal.	14-Oct-22
45438, 45456	Administrators were unable to configure Modern Authentication for the Outlook app through the App Config workflow.	25-Oct-22
45356	The data in the Deployment Overview report received via email subscription was misaligned.	28-Oct-22
45291	Administrators could not publish App Compliance policy settings without providing an app ID for the **Other System Apps to be Allowed**.	28-Oct-22

10.87 Release Fix Summary

The following customer issues were fixed in the 10.87 release:

Fix number	Description
44764	Fixed an issue with the API timestamp for the Admin Login report.
44820	Fixed an issue with the Error.Parsing Request failing after selecting Device > Enrollment.
44902, 44970	Fixed an issue with Android app wrapping failure after recompiling the app.
44958	Fixed an issue with the Forgot pin option not working for Android users.
44998	Fixed an issue where Android Enterprise users couldn't install apps.
45084	Fixed an issue where Maas360 admins could not publish a MaaS360 policy.
42432	Fixed an issue with bulk updating iOS policies.
43543	Fixed an issue where iOS app distribution and installation details weren't loading.
43813	Fixed an issue where bulk updates to an Android policy changed other settings.
44454	Fixed an issue where mobile configurations for macOS was failing and did not allow for full disk access to be enabled.
44676	Fixed an issue where the password reset message on the portal needed to be updated across all instances.
44685	Fixed an issue with the Remove on Stopping Distribution action not working properly on the portal.
44686	Fixed an issue where additional Office 365 user records were being added for some users.
44867	Fixed an issue with a large number of incomplete SSL handshake requests to https://login.maas360.com.
44966	Fixed an issue with the location name not appearing in Device history under comments when a policy was changed due to location changes.
45014	Fixed an issue where the admin received an error prompt during Android Device enrollment when tje admin unchecked 'enroll with MDM.'
45118	Fixed an issue where a policy was not updated on Android devices.
45163	Fixed an issue where the customer tried to export an Android policy, but received a blank page.
45222	Fixed an issue with app configurations for the Microsoft Outlook app on Android devices.
42572	Fixed an issue where multiple iOS policies were not changed even though customer enabled the 'Apply changes to more Policies' check box.

September 2022 Daily Fixes Summary

MaaS360 Daily Fixes - September 2022

Fix	Description	Date Released
45253	Users were unable to install iOS enterprise apps from the MaaS360 app catalog	02-Sep-2022
45263	An administrator could not override an already uploaded app config XML file with a new one.	12-Sep-2022
45271	When a location-based policy was assigned to a specific user group, the policy was auto-assigned to some users who were not part of that group.	14-Sep-2022
44749	When a policy was applied to a single device, administrators could not load the device view on clicking the **Applied to <> devices** option in the Policies list page.	15-Sep-2022
44956	Administrators were unable to create a device group using the advance search that was pre-populated on their MaaS360 Home page.	16-Sep-2022
45261	Administrators did not receive email notifications for the subscribed reports.	20-Sep-2022
45073	F5 Access app did not receive VPN configurations pushed through app configurations in the MaaS360 portal.	20-Sep-2022
45275	The App Configuration workflow was unavailable in the MaaS360 account, and the App Configuration section was unavailable for an app.	22-Sep-2022
45319	MaaS360 could not automatically renew user and device certificates.	21-Sep-2022

August 2022 Daily Fixes Summary

MaaS360 Daily Fixes - August 2022

Fix	Description	Date Released
45149	A web app remained on the device even though the app was deleted from the App Catalog in the MaaS360 portal.	04-August-22
45071	Exchange ActiveSync integration in Cloud Extender failed due to an error in the incremental sync in the Exchange Server.	18-August-22
45246	When attempting to enroll a DEP device, the enrollment of devices failed with **Invalid Profile** error or **Invalid Request Parameters** error.	31-August-22

July 2022 Daily Fixes Summary

MaaS360 Daily Fixes - July 2022

Fix	Description	Date Released
45018	After the enrollment, devices failed to report network payload to the MaaS360 portal on M3 instances.	04-July-22
44807	Users were able to remove a device through End User Portal (EUP) without requiring MaaS360 passcode.	05-July-22
44806	When adding an iTunes App Store app through the MaaS360 portal, the countries Democratic Republic of the Congo, Kosovo, and Nauru were not listed in the Region dropdown. As a result, administrators were unable to add an iTunes App Store App via MaaS360 App catalog to those countries.	06-July-22
44831	When a config file without an extension was pushed to internal device storage through Docs, MaaS360 automatically added a .unknown file extension. As a result, third-party apps were unable to read the file.	06-July-22
45042	After the enrollment, devices failed to report device summary data such as IMEI, Manufacturer, and OS to the MaaS360 portal on M3 instances.	11-July-22
44851	After migrating from Ping-One to ISV, the samAccountName attribute was not used as a username in the MaaS360 portal.	19-July-22
44941	Customers were unable to delete hidden/inactive devices from the MaaS360 portal.	22-July-22
45063	A configuration field was unavailable in app configurations for an Android Enterprise app.	25-July-22
45077	The default domain values configured in the MaaS360 Settings were not displayed in the Domain field during the enrollment.	26-July-22
45093	Administrators could not re-upload an iOS Enterprise app after deleting the app.	27-July-22
44923	When administrators tried to view exceptions in the Exceptions Report page, the View link did not load.	28-July-22
45016	The **Administrative access control** flag was greyed out, even though no administrators or distributions were configured for the groups.	29-July-22

June 2022 Daily Fixes Summary

MaaS360 Daily Fixes - June 2022

Fix	Description	Date released
44795	The app configurations that were uploaded in the old flow did not load after migrating to the new app configuration flow.	14-June-22
44935	The identity certificates were automatically removed on editing a policy, and those certificates were removed on devices on publishing that policy.	16-June-22
44818	Reports from App Inventory in Device Details were missing columns when exported.	16-June-22
44596	After migrating Device Admin devices to Android Profile Owner mode, the enrollment e-mail client shows as a separate device record.	21-June-22
44169	There was a discrepancy between the count of devices shown in UEM Overview report and the Device inventory page.	22-June-22
44752	A newly added Azure user was deactivated on each sync.	22-June-22
44941	Hidden/Inactive devices were not being deleted from the portal after 24 hours.	22-June-22
44730	The App Inventory report displayed an error message when administrators tried to generate **Installs by App Version** and **App Installs by OS Version** reports for an OEM Config app.	24-June-22
44734	The document that was distributed from the portal was not available on the device.	28-June-22
44951	Policy publish failed with an error message even though the corresponding values were selected in the VPN profile.	29-June-22
44756	When administrators tried to view exceptions in the Exceptions Report page, the View link on page 2 does not navigate them to the third page.	30-June-22

10.86 Release Fix Summary

The following customer issues were fixed in the 10.86 release:

Fix number	Description
43892	Fixed an issue where Android MDM policies that were scheduled for bulk edit failed to publish if multiple permissions were configured for a single app ID.
44679	Fixed an issue where administrators could not deploy iOS public apps and iOS web apps in a single distribution to a specific iOS device.
44225	Fixed an issue with MaaS360 Portal slow response times on M4 accounts.
44511	Fixed an issue where MaaS360 advanced search exports blank spreadsheet with only headers when FileVault Recovery Key Present is included in the search criteria.
44706	Fixed an issue where the More option under the device name on the Device Inventory view was not displaying the correct page.
44714	Fixed an issue where the list of Cloud Extenders was not loading when the administrator accessed Setup > Cloud Extender.
44736	Fixed an issue where the MaaS360 app prompted the customer to enter their 4-digit passcode instead of their corporate password.
44331	Fixed an issue where the customer was not receiving an email after creating a report subscription.
44397	Fixed an issue with the primary admin listed in the Accounts tab for the customer.
44484	Fixed an issue where the User Password Link email was not sent when the Local User was created from the API.
44504	Fixed an issue with a page hanging after saving a group of devices.
44567	Fixed an issue with an iOS device not being enrolled in SPS mode.
44572	Fixed an issue where enforcement rules changed a policy even though the Application Compliance configuration was different between policies.
44578	Fixed an issue where the MaaS360 Portal was displaying garbled Japanese text when the criteria of device groups were created in an earlier platform release.
44611	Fixed an issue with G Suite SAML failing.
44717	Fixed an issue where Android devices were being prompted for a 4-digit passcode in the MaaS360 app instead of the LDAP password.
44837	Fixed an issue with a passcode error after the administrator set the Portal login for SSO from Duo.
44343	Fixed an issue where updated user record attributes from an API call to update MailDomain were being reverted back after 24 hours.
44408	Fixed an issue where Advanced Search wasn't exporting data correctly.
44487	Fixed an issue where the More link in the MaaS360 Portal wasn't showing menu options.
44508	Fixed an issue where the number filter at the bottom of the Actions and Event workflow (Devices > Actions & Events) was showing NaN (Not a Number) instead of the actual number.
44509	Fixed an issue where creating a new policy showed placeholder text instead of the actual policy name.
44641	Fixed an issue with Bulk User Upload formatting that previously worked.
44772	Fixed an issue with the Learn More link that was broken for an IBM ID linking to admin accounts.

May 2022 Daily Fixes Summary

MaaS360 Daily Fixes - May 2022

Fix	Description	Date Released
44777	Administrators were unable to upload an enterprise app of type Packages for Windows in the App Catalog.	20-May-22
44636	Administrators were unable to sync Azure AD groups to MaaS360.	20-May-22

April 2022 Daily Fixes Summary

MaaS360 Daily Fixes - April 2022

Fix	Description	Date Released
44366	Apple devices did not receive the default MDM policy after enrolling through DEP.	05-April-22
44052	The PC Inventory Software report did not display existing filter options when subscribing for Email Delivery.	07-April-22
44520	Newly enrolled iOS 15 devices did not receive the VPN policy that consisted of the list of apps that were allowed to use VPN.	07-April-22
44600	Customers could not log in to IBM Security Verify portal through MaaS360.	07-April-22
44570	Administrators were unable to deploy iOS updates to device groups.	08-April-22
43277	Android devices enrolled in DO mode did not receive the latest version of an Android enterprise app.	08-April-22
43586	Administrators who subscribed to UEM Overview report did not receive the report to the configured email address.	13-April-22
43508	Administrators could not generate Mobile Data Usage Analysis reports in the MaaS360 portal.	22-April-22
44598	When adding an iTunes App Store app through the MaaS360 portal, the country Bosnia and Herzegovina was not listed in the region dropdown.	25-April-22
44293	Enterprise Email Integration for G-Suite stopped syncing new devices to the MaaS360 portal.	27-April-22
44635	Biometric unlock was disabled and users could not change biometric settings on the device.	27-April-22
44576	A blank white screen was displayed when administrators tried to release VPP licenses from a device	28-April-22

10.85 Release Fix Summary

The following customer issues were fixed in the 10.85 release:

Fix number	Description
43923	Fixed an issue where device enrollments were failing if the license type wasn't set automatically.
43696	Fixed an issue with the Device Name column in custom reports.
43963	Fixed an issue where the user was unable to set app configuration for a specific app.
43951	Fixed an issue where the MSP master account was not showing the correct account information after a timeout.
44073	Fixed an issue with garbled Japanese text in the [Department/Business Unit] field in device inventory.
44099	Fixed an issue where the user was receiving an error when they clicked Device Details in a report.
44442	Fixed an authentication issue with the user logging in to the end-user portal.
38252	Fixed an issue that restricted admins from viewing My Alert Center on all devices.
43619	Fixed an issue with changing policies on macOS machines.
43688	Fixed an issue where a new admin was not receiving a temp password to log in to the portal.
43828	Fixed an issue where the macOS wifi profile kept disconnecting and required a password every time a macOS device restarted.
44192	Fixed an issue where the admin could not delete/remove alerts from My Alert Center.
43867	Fixed an issue where the admin could not generate an installed software inventory report.
43985	Fixed an issue where there was no option for IP address under network information on the Advanced Search page.
44096	Fixed an issue where the portal was not updating custom attribute values in the device inventory when Japanese was selected.
44143	Fixed an issue where the customer was receiving email alerts from the portal containing Chinese characters.
44204	Fixed an issue where the term 'whitelist' was still displayed in the WorkPlace Persona policy settings.
44225	Fixed an issue where the customer was receiving slow portal response times when logging into their M4 accounts.
44348	Fixed an issue where the per app VPN payload for the iOS MDM policy failed to install.
43600	Fixed an issue where 'Bulk Add' failed if the CSV file contained an Access Control policy.
43959	Fixed an issue where Chrome was not detected as an OS type in the Administrators Logins report.
44228	Fixed an issue with incorrect Japanese translations in the Add Device workflow for License Management.
44297	Fixed an issue where customers could not view details under Device Summary > App Distributions > App Distributions Details.
43563	Fixed the syntax of the wildcard from ***.*domainname.com*** to ***.*domain.**** that is displayed in the help text below the Android Enterprise policies > Configure Allowed Accounts (Allowlist).
43738	Fixed an issue where administrators were unable to upgrade an Android enterprise app in the Maas360 portal.
44249	Fixed an issue where devices were enrolled in the Device Admin mode instead of the Profile Owner mode.

March 2022 Daily Fixes Summary

MaaS360 Daily Fixes - March 2022

Fix	Description	Date Released
44171	Android devices did not receive the latest policy version from the MaaS360 portal.	07-Mar-2022
44522	Administrators were unable to log into the MaaS360 portal and users were unable to authenticate device enrollments with Azure credentials.	15-Mar-2022
44410	MDM policy was changed on iOS devices and administrators were unable to apply the original policy to those devices.	21-Mar-2022
44381	References to racially insensitive terminology such as Blacklist/Whitelist was found in Windows MDM policies > Device Settings > Advanced App Compliance.	22-Mar-2022
44053	The PC Inventory Software Report Custom Filter name with space shows junk characters (%@x20) instead of the actual space.	22-Mar-2022
41435	Administrators were unable to view custom filters they created in the Reports workflow.	22-Mar-2022
44526, 44452	Some workflows in the MaaS360 portal (For example - Device Inventory) were loading slowly or irresponsive.	22-Mar-2022
44473	When the administrators assigned a policy to iOS devices, MaaS360 changed the policy back to the default policy.	22-Mar-2022
44260	The **Delete Device** option was unavailable for an inactive device.	22-Mar-2022
118326	An invalid date was displayed in Next Mail schedule for subscription hardware inventory reports.	23-Mar-2022
44194	Samsung was not listed in the **Reports** > **App inventory** > **Overview** > **Total Apps installed by Device Manufacturer** workflow.	25-Mar-2022
44380	Inactive devices were still displayed in the MaaS360 portal 24 hours after administrators deleted those records.	30-Mar-2022
44427	The option to set maximum number of devices allowed to enroll in to MaaS360 account was unavailable for customers in the Advanced Device Enrollment Settings.	30-Mar-2022
44496	When configuring a Box certificate in Docs > Content Sources, the Submit button was unavailable in the MaaS360 portal.	30-Mar-2022
44327	When a user tried to change the From Date of a Calendar event, MaaS360 displayed a transparent background for the overlaid calendar, making it difficult for users to select a new date.	30-Mar-2022
44554	A web app was active on devices even though it was deleted in the MaaS360 App Catalog.	30-Mar-2022

February 2022 Daily Fixes Summary

MaaS360 Daily Fixes - February 2022

Fix	Description	Date Released
44258	After setting up Okta integration for user authentication, users were redirected to the IBM MaaS360 login page instead of the Okta login page.	04-Feb-2022
44210	When adding an iTunes App Store app through the MaaS360 portal, Serbia was not listed in the region dropdown.	07-Feb-2022
43774	When a user's email address was updated in the Active Directory, the changes were not reflected on the Device Summary page (Devices>Inventory).	07-Feb-2022
44298	Administrators could not deploy enterprise apps to Android devices.	08-Feb-2022
44291	The options to create an Android MDM policy were unavailable in the MaaS360 portal for new customers.	14-Feb-2022
43764	New device enrollments failed to auto-approve even though Auto-Quarantine and auto-approval of devices were enabled in the Cloud Extender policy settings.	14-Feb-2022
42001	Gateway timeout error message was displayed when administrators tried to export device inventory from the MaaS360 portal.	14-Feb-2022
44356	A blank screen was displayed when users tried to reset the PIN for the MaaS360 for Android app.	17-Feb-2022
44279	An error message was displayed when administrators tried to distribute a folder path via Windows file share.	17-Feb-2022
44351	Administrators could not deploy enterprise apps to Android devices. The app distribution was stuck at the Downloading state.	21-Feb-2022

January 2022 Daily Fixes Summary

MaaS360 Daily Fixes - January 2022

Fix #	Description	Date Released
43960	Administrators could not generate an App Inventory report to retrieve Device Details for an app in the MaaS360 portal.	06-Jan-2022
44056	The user data was not displayed on the user view page if the user custom attributes were configured with the (/) symbol.	06-Jan-2022
43713	The storage data is missing in the Hardware Inventory report.	11-Jan-2022
44066	When a device merge action was performed via **Devices** > **Exceptions** workflow, the page darkens and the action does not complete.	13-Jan-2022
43908	When Install Automatically was selected on the App Summary page, the page became unresponsive.	18-Jan-2022
43686	An iOS Enterprise app could not connect to the database server.	19-Jan-2022
44105	An incorrect app icon was displayed for the Android app version 7.71 in the MaaS360 portal > App Catalog.	19-Jan-2022
43948	After enrollment, devices were displayed in the correct enrollment group, but users had to wait up to 15 minutes before app distributions were processed on devices.	20-Jan-2022
43996	Administrators could not publish an app configuration for the Samsung Smart Switch Mobile app.	27-Jan-2022
44208	The default Android policy was not applied to the devices after the enrollment.	28-Jan-2022
44251	The DEP enrollments that require authentication against AD/AzureAD authentication could not be processed.	31-Jan-2022

10.84 Release Fix Summary

The following customer issues were fixed in the 10.84 release:

Fix number	Description
43606	Fixed an issue where the admin was unable to launch the Setup > Administrator page.
41566	Fixed an issue where the admin was unable to search for a Zebra device after enrolling the device in the portal.
43159	Fixed an issue where the macOS shell script was not executing.
43261	Fixed an issue where the admin was unable to add Windows.exe apps to the MaaS360 platform.
43569	Fixed an issue where clicking the "Add User" button in the upper right corner of the portal home page incorrectly inserted a compliance table.
43646	Fixed an issue where OEMConfig was not applied to devices during app distribution.
43649	Fixed an issue where the admin received an error message while enrolling Android devices in DO mode.
43769	Fixed an issue with the Exchange ActiveSync payload not installing on iOS devices.
43809	Fixed an issue with iOS VPP apps not installing.
43881	Fixed an issue with devices not being reclassified from inactive to active as expected.
40947	Fixed an issue with host pairing not working on iOS 13+ devices.
42636	Fixed an issue where the admin was unable to access an iOS 14.4.2 DEP supervised device, with a DEP Profile that had Allow Pairing unchecked, from iTunes with the Allowing Host Pairing MDM policy.
42714	Fixed an issue where the customer was getting stuck during initial portal setup (during quick start).
42750	Fixed an issue with the Wandera app not automatically re-installing when re-added to a Group that had Wandera as a pushed app.
42866	Fixed an issue where the admin was not receiving enrollment emails after trying to enroll their test device.
43074	Fixed an issue where a policy was failing email login authentication for new enrollments.
43334	Fixed an issue where auto device naming was not functioning for multiple iOS devices.
43414	Fixed an issue where the admin was experiencing delays when trying to apply OEMConfig settings on Android Enterprise devices.
43422	Fixed an issue where the admin could not create a Google account during Knox enrollment.
43484	Fixed an issue with the Expense Management Plan not being applied to individual devices after being applied through Device Groups.
43486	Fixed an issue where the admin was unable to add a new admin to the portal.
43581	Fixed an issue with the incorrect app version being installed on devices.
43674	Fixed an issue where after enabling "License Management" for the account, enrollment by local authentication was not completing after authentication.
43765	Fixed an issue where text in a Android Enterprise Security policy setting was out of place.
43829	Fixed an issue where the portal was not allowing users to use iOS dictation.
43856	Fixed an issue where the admin couldn't change a ruleset message.
43870	Fixed an issue where the admin couldn't create a web apps approval template.
41691	Fixed an issue where the portal user interface still displayed a deprecated service, IBM Connections Cloud.
43580	Fixed a misspelled word in an iOS policy.

December 2021 Daily Fixes Summary

MaaS360 Daily Fixes - December 2021

Fix #	Description	Date Released
43885	Android devices did not report the Last reported data to the MaaS360 portal.	02-Dec-2021
44012	The error message **Device registration request failed** was displayed and the enrollment of Android devices failed.	08-Dec-2021
44064	The bulk enrollment of Bluebird devices in the Device Admin mode failed.	20-Dec-2021
43976	MaaS360 displayed an incorrect folder structure wherein Deleted items were displayed in the root folder instead of the All Folders list in the Secure Mail app.	23-Dec-2021
44111	The distribution of Android app version 7.71 was stuck at the Pending Update state.	23-Dec-2021

iOS Release Summaries

MaaS360 iOS Release Summaries

iOS SDK and Wrapping 4.40 Release Summary

MaaS360 makes the iOS SDK and Wrapping version 4.40 available on 20 December 2022.

Defect	Summary
45052, 45619	Customers were unable to perform wrapping on the app via MaaS360 if the SDK app is built with iOS 13.3 and above.

Secure Browser 3.90 Release Summary

MaaS360 makes the iOS Secure Browser app version 3.90 beta available on TestFlight on 27 October 2022.

Discontinued support for iOS 13 >>

The Secure Browser app version 3.90 is no longer supported on devices running iOS version 13 and lower. The minimum OS requirement for the Secure Browser app version 3.90 is now iOS 14. The end of support implies that users running versions older than iOS 14 cannot download the Secure Browser app version 3.90 from the App Store. MaaS360 recommends customers to upgrade to the supported OS versions to take advantage of future Secure Browser app versions.

Secure Editor 3.20 Release Summary

MaaS360 makes the iOS Secure Editor app version 3.20 beta available on TestFlight on 27 October 2022.

Discontinued support for iOS 13 >>

The Secure Editor app version 3.20 is no longer supported on devices running iOS version 13 and lower. The minimum OS requirement for Secure Editor app version 3.20 is now iOS 14. The end of support implies that users running versions older than iOS 14 cannot download Secure Editor app version 3.20 from the App Store. MaaS360 recommends customers to upgrade to the supported OS versions to take advantage of future Secure Editor app versions.

User Interface enhancements >>

The updated Secure Editor app features a redesigned document detail view and other productivity improvements.

iOS 5.30 Release Summary

MaaS360 makes the iOS app version 5.30 beta available on TestFlight on 27 October 2022.

PDF Form support >>

MaaS360 upgrades the PSPDFKit library to allow users to easily view, edit, and save PDF Form data.

Note: MaaS360 does not support Signature field in PDF Forms.

Discontinued support for iOS 13 >>

MaaS360 app version 5.30 is no longer supported on devices running iOS version 13 and lower. The minimum OS requirement for MaaS360 app version 5.30 is now iOS 14. The end of support implies that users running versions older than iOS 14 cannot download MaaS360 app version 5.30 from the App Store. MaaS360 recommends customers to upgrade to the supported OS versions to take advantage of future MaaS360 app versions.

MSAL SDK Upgrade >>

MaaS360 upgrades MSAL SDK version from 1.1.26 to 1.2.2.

Defect Fixes

Defect	Summary
45237	The mail content was not displayed intermittently after migrating the email server to Google Workspace.
45544	The Search option was unavailable in the PDF files on MDM enrolled devices.
45460, 45366	Email and Calendar sync improvements.

iOS 5.21 Release Summary

MaaS360 makes iOS app version 5.21 available on App Store on 19th October 2022.

Defect Fixes

Defect	Summary
45325	Users were unable to send files and photos to the MaaS360 Secure Mail app via Share extension.

iOS SDK and Wrapping 4.35 Release Summary

MaaS360 makes the iOS SDK and Wrapping version 4.35 available on 09 September 2022.

Defect	Summary
44309	A wrapped app could not complete the activation after switching to the MaaS360 app.

iOS Secure Browser 3.80 Release Summary

MaaS360 makes the Secure Browser version 3.80 available on App Store on 13 September 2022.

Discontinued support for iOS 12 >>

The Secure Browser app version 3.80 is no longer supported on devices running iOS version 12 and lower. The minimum OS requirement for Secure Browser app version 3.80 is now iOS 13. The end of support implies that users running versions older than iOS 13 cannot download Secure Browser app version 3.80 from the App Store. MaaS360 recommends customers to upgrade to the supported OS versions to take advantage of the future Secure Browser app versions.

iOS 16 Zero day support >>

MaaS360 announces zero-day support for iOS 16. With this support, the Secure Browser app works seamlessly on iOS 16 devices without any disruption.

Defect Fixes

Defect	Description
44866	Users were unable to connect to intranet sites through MaaS360 Secure Browser after configuring Mobile Enterprise Gateway (MEG) module.
45017	After connecting to Mobile Enterprise Gateway (MEG), users were unable to download files through Secure Browser in scenarios where filename was missing in the HTTP header.
44883	When users launch the Secure Browser app from the background, the gateway connection times out and the device does not start MEG connection until users manually tap **Retry**. To allow the devices to automatically re-establish MEG connection, follow these steps: 1. Open the Persona policy. 2. Navigate to **WorkPlace** > **Security**. 3. Provide the following key value pair in **Advanced Configuration Details**. • Key: ***BrowserOnForegroundConnectVPNMEG3*** • Value: ***Yes***

iOS 5.20 Release Summary

MaaS360 makes iOS app version 5.20 available on App Store on 13 September 2022.

Discontinued support for iOS 12 >>

MaaS360 app version 5.20 is no longer supported on devices running iOS version 12 and lower. The minimum OS requirement for MaaS360 app version 5.20 is now iOS 13. The end of support implies that users running versions older than iOS 13 cannot download MaaS360 app version 5.20 from the App Store. MaaS360 recommends customers to upgrade to the supported OS versions to take advantage of future MaaS360 app versions.

iOS 16 Zero day support >>

MaaS360 announces zero-day support for iOS 16. With this support, new iOS 16 devices can enroll with MaaS360, and existing devices upgrading to iOS 16 continue to work seamlessly without any disruption.

Changes to the device name for devices activated in MaaS360 >>

To protect the end-user's privacy, iOS 16+ devices that are activated in MaaS360 no longer share user-assigned device name (General > About > Name) with the MaaS360 portal. As a result, MaaS360 uses the combination of MaaS360 username and Device type separated by a hyphen as a device name for the SPS activated devices.

MaaS360 uses the following format to generate the device name for activated devices running iOS 16 and later:

<username>-<device model>

Example:

iOS 15 and earlier	iOS 16 and later
Denise’s iPhone 13 Pro	denise-iPhone

Note: There is no impact to the device name for MDM enrolled devices.

Defect Fixes

Defect	Summary
S-153820	EWS push notifications played sound when the device was in silent mode.
45103	An incorrect password error was displayed when administrators tried to open password-protected device log zip files that were gathered from the MaaS360 portal.
45220	The Inbox dropdown overrides with the tick mark icon in the Secure Mail app after changing the orientation from landscape to portrait on iOS 16 devices.
45218	A blank white space was displayed in the email preview pane when emails were selected in the Secure Mail app on iOS 16 devices.

iOS SDK and Wrapping 4.30 Release Summary

MaaS360 makes the iOS SDK and Wrapping version 4.30 available on 30 July 2022.

Defect Fixes

Defect	Summary
39622	After turning on the certificate pinning, if an SDK app was inactive for a long time, the certificates were revoked, and the error message Untrusted connection was displayed when users opened the app.

iOS Secure Browser 3.70.5 Release Summary

MaaS360 makes Secure Browser app version 3.70.5 available on iTunes on 19 May 2022.

Defect Fixes

Defect	Description
43916	The gateway requests from the devices failed to reach the gateway server, resulting in the MaaS360 Secure Browser app crashes.

iOS 5.10 Release Summary

MaaS360 makes iOS app version 5.10 beta available on TestFlight on 09 June 2022.

MaaS360 app automatically uses the latest Exchange ActiveSync (EAS) protocol if users upgrade to EAS 16 >>

In the previous releases, administrators had to enable the use of EAS 16 protocol on end-user devices through an advanced configuration parameter in the Security policies.

Effective MaaS360 for iOS app version 5.10 release, if an upgrade to EAS 16 is available for the device, MaaS360 app will automatically use the EAS 16 protocol and starts syncing mails, calendar, and contacts in the background. Because the MaaS360 app version 5.10+ automatically uses EAS 16, the prompt to enable the use of EAS 16 will not be displayed to the end-users.

Customer impact

- All emails will be re-synced from the Exchange server. However, the previously downloaded email attachments must be re-downloaded.
- The re-sync process may show empty mail list temporarily until MaaS360 app starts syncing new mails from the Exchange server.
- The re-sync process might block UI touch events for a few seconds while cleaning up previously downloaded emails.

Note: There is no impact to existing accounts that have the EAS 16 protocol enabled through advanced configuration settings in Security policies.

Defect Fixes

Defect	Summary
44665	Badge count was not displayed and new email notifications were not delivered even though subscription-based email notifications setting was enabled.
54816	The following error message was displayed during the enrollment and activation of devices. Cert pinning error message
44803	When a reoccurring or single calendar appointment was forwarded from one user to another, the email body was blank at the recipient's end.
44862	When replying to an email, the Secure Mail app did not display From, Date, To, and Subject fields.

iOS Secure Editor 3.10.18 Release Summary

MaaS360 makes the iOS Secure Editor app version 3.10.18 available on TestFlight on 10 May 2022.

- Secure Editor upgrades zlib to version 1.2.12.

iOS Secure Editor 3.0 Release Summary

MaaS360 makes the iOS Secure Editor app version 3.0 available on iTunes on 27 April 2022.

- Secure Editor upgrades its OpenSSL library to version 1.1.1m.

Defect Fixes

Defect	Summary
43521	Users could not save Windows File Sharing files to the source in Secure Editor.

iOS MaaS360 VPN 3.22.1 Release Summary

MaaS360 makes the VPN app version 3.22.1 available on the iTunes app on 20 April 2022.

- MaaS360 adds a fix to support TCP mode of MaaS360 VPN server and makes changes to the client configuration that are required to establish a connection with the MaaS360 VPN in the TCP mode.

iOS 5.0 Release Summary

MaaS360 makes the iOS app version 5.0 available on the iTunes app on 06 April 2022.

MaaS360 upgrades zlib to version 1.2.12.

Defect Fixes

Defect #	Summary
44367	If the pdf file had a comma in the filename, the pdf file was split into two files when imported into MaaS360.
44342	Users could not sign in to the MaaS360 app on DEP devices.
44283	The activation of iOS devices through a QR code failed with the "Enrollment Request Invalid" message.
44136	The certificate pinning failed on devices due to an unsupported algorithm in the customer certificate.
44227	iOS devices were unable to play MP3 attachments that were received via emails on the Secure Email app.

iOS SDK and Wrapping 4.20.000 Release Summary

MaaS360 makes the iOS SDK and Wrapping version 4.20.000 available on 23 March 2022.

Defect Fixes

Defect	Summary
44306	Users had to restart iOS Enterprise apps to reconnect to MaaS360 Mobile Enterprise Gateway (MEG).
44305	iOS Enterprise apps did not load the UI labels on the login screen.

iOS 4.92.4 Release Summary

MaaS360 makes the iOS app version 4.92.4 available on iTunes on 4th March 2022.

MaaS360 upgrades its OpenSSL library to version 1.1.1m.

iOS 4.91 Release Summary

MaaS360 makes the iOS app version 4.91 available on the iTunes app on 22 January 2022.

Defect fixes

Fix #	Description
44232	When the administrators deployed a certificate, users were unable to download the certificate on the devices and the configuration of certificates on the MaaS360 app failed.

iOS SDK and Wrapping 4.10 Release Summary

MaaS360 makes the iOS SDK and Wrapping version 4.10 available on 19 January 2022.

Defect Fixes

Fix #	Description
44074, 43686	The VPN setting was automatically turned off on iOS devices. As a result, the SDK apps failed to connect to MaaS360 Enterprise Gateway (MEG).

iOS 4.90 Release Summary

MaaS360 makes the iOS app version 4.90 available on iTunes on 17 January 2022.

Defect fixes

Defect #	Summary
43623	When the subscription-based notifications are enabled through WorkPlace persona policies, the MaaS360 for iOS app crashed after signing in to the Secure Mail account.

Android Release Summaries

MaaS360 Android Release Summaries

Android 8.10 Release Summary

MaaS360 makes the Android app version 8.10 beta available on Play Store on 28 November 2022.

New enhancements to Android agent enrollment workflows >>

In Android app version 8.0, MaaS360 revamped Android agent enrollment screens with a new user interface and productivity enhancements. In the previous releases, the new enrollments enhancements were available only to Device Admin bulk enrollments by default. Administrators had to create and embed a custom URL in the HTML file to apply new enrollment changes to Profile Owner, Device Admin, and SPS.

MaaS360 adds the following enhancements in Android app version 8.10:

- Extends new enrollment enhancements to all the enrollment modes (Device Admin, Profile Owner, and Device Owner). All devices automatically go through the new enrollment flow during the enrollment without requiring additional configuration.
- Allows administrators to force the device enrollment as a part of device provisioning so that users cannot skip important device enrollment screens.
- Replaces local authentication screens with a unified webview.
- Removes enrollment completion notification and displays the enrollment status directly on the enrollment screen.
- Displays the number of retry attempts directly on the enrollment screens.

Note: New enrollment screens are available only on devices running Android OS version 7 and later. Requires MaaS360 for Android app version 8.10.

Android OS versions 5 and 6 is no longer recommended by MaaS360 >>

In Q1 2022, MaaS360 announced the end of support timelines and then constantly reminded customers to target devices running Android OS versions 5 and 6 for OS upgrade or replacement. Effective with MaaS360 agent version 8.10, devices that run these OS versions will no longer receive new MaaS360 apps. The MaaS360 agent app version 8.05 is the last supported version for devices running OS versions 5 and 6. If there are issues or bugs with OS versions 5 and 6, customers cannot raise support tickets for problems that occur on these OS versions.

Customer impact on devices running OS versions 5 and 6:

- Devices that are currently enrolled can continue to be enrolled and secured until further notification. These devices are automatically locked to the MaaS360 app version 8.05.
- New devices can be enrolled with MaaS360 app version 8.05, which is the last supported agent version on unsupported devices.
- Effective with MaaS360 SDK version 8.10, MaaS360 freezes support for these older versions. The minimum OS version requirement for the MaaS360 SDK jar 8.10 is Android 7 and later.
- The apps that are wrapped or updated after the 10.88 release are compatible only on Android devices running OS versions 7 and later. Existing apps continue to work on older OS versions unless they are updated or re-wrapped after the 10.88 release. If customers want to manage both existing and new apps, the apps wrapped after 10.88 release must be added as an additional version.

End of support announcement for Knox enrollments on Android OS version 7 >>

Samsung announced the end of support for Knox enrollments on Android OS version 7 in the policy update statement. As per the policy update, Samsung updated the minimum supported versions to restrict Knox enrollments to Android OS versions Android 8.0 (Knox 3.0) and later. For more information on the policy update, see https://www.samsungknox.com/en/blog/policy-update-on-knox-supported-versions.

To comply with Samsung's policy update requirements, MaaS360 no longer supports Samsung Knox enrollments (new/re-enrollment) on Android OS version 7 effective with MaaS360 for Android app version 8.10.

Impact:

- Existing devices - Android 7 devices that are already enrolled into MaaS360 are unaffected, but they will not be able to re-enroll.
- New devices - Android 7 devices can no longer enroll with MaaS360 for Android app version 8.10.

Updated messaging in the MaaS360 for Android app to improve end-user transparency >>

MaaS360 improves messaging in some permission request and dialog boxes that are presented in the MaaS360 for Android app based on Google's privacy policies.

MaaS360 adds the following enhancements:

- Updated permission dialogs based on Google's best practices to make permissions more understandable, useful, and secure for users. The updated permission dialogs clearly explain what data the MaaS360 app is trying to access and what benefits the app can provide to the users if they grant that permission. In scenarios where the permission is critical to the functioning of the MaaS360 app, MaaS360 displays a rationale screen to explain why the permission is required and what functionalities are affected if the permission is denied.
- When users try to remove MDM control, MaaS360 presents an additional dialog that clearly explains the functionality impact so that users can take

informed decisions.
- Displays the list of all the policies that are enforced by the organization to manage devices.

Configure time for the kiosk device to return to the single app mode >>

MaaS360 adds a new policy setting to allow administrators to configure the time before the configured app is automatically launched when users exit the single app mode. Users exit the single app mode to perform activities such as changing device settings and checking the billing ID. In the previous releases, the timer was automatically set to 60 seconds by default. If this setting is not configured, the configured app is automatically launched 60 seconds after users exit the single app mode.

Note: Supported only for the single app mode. COSU Mode Type must be set to **Automatically launch a required app and lock the device to display only this**.

Path: **Android Enterprise settings** > **COSU (Kiosk mode)** > **Time after which app should be launched automatically (in seconds)**.

Android 8.05 Release Summary

MaaS360 makes Android app version 8.05 available on Play Store on 15 November 2022.

MaaS360 Docs app no longer uses REQUEST_INSTALL_PACKAGES permission >>

To comply with Google Play policies, MaaS360 no longer requires REQUEST_INSTALL_PACKAGES permission for the Docs app.

Impact: Users cannot install the .apk files distributed by the administrators via the Docs app. As an alternative, administrators can use MaaS360 App Catalog to distribute .apk files to devices.

New enrollment workflow changes now available for DA and PO enrollments by default >>

In MaaS360 for Android app version 8.0, MaaS360 redesigned the Android agent enrollment screens and made the new enrollment enhancements available to Device Admin bulk enrollments available by default. In previous releases, administrators had to create and embed a custom URL in the HTML file to apply new enrollment changes to Profile Owner, Device Admin, and SPS. Effective with MaaS360 for Android app version 8.05, MaaS360 turns on new enrollment changes for Profile Owner, Device Admin, SPS, and Device Owner (token-based) enrollments. With this support, the new enrollment changes are now available to Profile Owner, Device Admin, SPS, and Device Owner (token-based) enrollments by default without requiring additional configuration.

For more information, see https://www.ibm.com/support/pages/node/6616243.

Android 8.01 Release Summary

MaaS360 makes Android app version 8.01 available on Play Store on 03 October 2022.

Defect Fixes

Defect	Summary
45225	Administrators could not initiate remote control using the Remote Support app on Samsung SM-A336E models.

Android 8.0 Release Summary

MaaS360 makes Android app version 8.0 beta available on Play Store on 29 August 2022.

Refactoring of Android agent enrollment workflows >>

MaaS360 redesigns Android agent enrollment screens to enhance the user experience and streamline the enrollment steps. As a part of design refactoring, MaaS360 adds granular enrollment steps and improves error handling.

Highlights:

- Completes device enrollment as a part of device provisioning
- Fixes issues with Zero-touch parameters.
- Optimizes retry logic.
- Resumes enrollment after restart from where it left off.
- Displays a uniform error screen across all steps in the enrollment flow, with support to Retry and Abort.
- Displays the enrollment stages with the help of labels/titles, allowing users to easily track the progress of the enrollment.

Deprecation of Basic Authentication in Exchange Online and G Suite >>

Microsoft announced they are turning off Basic Authentication for legacy protocols: Exchange Active Sync (EAS), Post Office Protocol (POP), Internet Message Access Protocol (IMAP), and Remote PowerShell (RPS) in Exchange Online. The adoption of Modern Authentication is the only path forward for the existing Exchange Online customers leveraging Basic Auth.

Android 13 Zero-day support

MaaS360 announces zero-day support for Android 13. With this support, new Android 13 devices enroll with MaaS360, and existing devices upgrading to Android 13 continue to work seamlessly without any disruption. MaaS360 ensures that both IT and end-users take advantage of new features built into Android's updated OS from the day of release.

- **Notification runtime permission >>**

  Android 13 introduces a new runtime notification permission, allowing users to focus on the notifications that are most important to them. The notification permission is turned off by default on Android 13 devices. Apps that are installed on Android 13 devices (or devices that upgraded to Android 13) will now request the notification permission before posting notifications. Users must explicitly grant the permission for the notifications to work. For Android Enterprise devices, MaaS360 automatically grants notification permission to core app, PIM, Docs, Browser, VPN, and Remote control. Administrators can use Android Enterprise policies to remotely control notification permission on the managed apps, and also to block apps that use the notification permission on managed devices. For device admin and SPS activated devices, users must explicitly grant notification permission for MaaS360 first-party apps from the corresponding app.

Android OS version 5 and 6 will no longer recommended by MaaS360 >>

MaaS360 does not recommend running devices on Android versions 5 and 6. MaaS360 will drop support for these OS versions with MaaS360 for Android app release 8.10, which is scheduled to be released in Q4.
In case there are issues or bugs, customers cannot raise support tickets for problems that occur on these OS versions. Customers can still raise tickets if they occur on later versions of the Android OS. But, these devices cannot receive bug fixes that are released with agent releases from October 2022.

Enhancements to Office 365 account sign out screen >>

MaaS360 displays the sign in information such as sign-in date, sign in app, sign in type in the MaaS360 Settings > Office 365 Accounts screen for Modern authentication-enabled Office 365 accounts.

Direct boot reset passcode support for Samsung devices >>

MaaS360 adds support to issue the reset passcode command to Samsung devices running 11+ when they are in the Direct boot mode.

Defect fixes

Defect	Summary

Defect	Summary
44970, 46793	The following error message was displayed when wrapping an app if android:extractNativeLibs was set to false in the AndroidManifest.xml file. To avoid the error message, administrators must set the following app wrapping parameter to true. • enableExtractNativeLib See https://www.ibm.com/docs/en/maas360?topic=wrapping-android-app-parameters
44969	The Wi-Fi icon changed to Android green icon on changing the language preferences in the Kiosk launcher.
44943	When admins configured attribute-based group assignment, the group membership failed and devices reverted to the default policy.
42785	A device reported Secure Browser app as an installed service, even though administrators did not deploy the app through policies.

Android 7.95 Release Summary

MaaS360 makes Android app version 7.95 beta available on Play Store on 25-July-2022.

Android 13 Zero-day support

MaaS360 announces zero-day support for Android 13. With this support, new Android 13 devices enroll with MaaS360, and existing devices upgrading to Android 13 continue to work seamlessly without any disruption. MaaS360 ensures that both IT and end-users take advantage of new features built into Android's updated OS from the day of release.

- **Notification runtime permission >>**

  Android 13 introduces a new runtime notification permission, allowing users to focus on the notifications that are most important to them. The notification permission is turned off by default on Android 13 devices. Apps that are installed on Android 13 devices (or devices that upgraded to Android 13) will now request the notification permission before posting notifications. Users must explicitly grant the permission for the notifications to work. For Android Enterprise devices, MaaS360 automatically grants notification permission to core app, PIM, Docs, Browser, VPN, and Remote control. Administrators can use Android Enterprise policies to remotely control notification permission on the managed apps, and also to block apps that use the notification permission on managed devices. For device admin and SPS activated devices, users must explicitly grant notification permission for MaaS360 first-party apps from the corresponding app.

- **End of Life for Kiosk Mode on Standard Device Admin Devices >>**

  Google deprecated legacy Device Admin for enterprise use effective with the Android 10 Q release. As a part of this deprecation, a number of Device Admin APIs are removed from support over time. To promote the adoption of Android Enterprise mode, MaaS360 stops supporting Kiosk mode on Standard Android 13 (non-Samsung) devices.

  Impact:

  - Kiosk policies are not supported and administrators cannot enable Kiosk for Device Admin devices.
  - The options to launch Kiosk mode are unavailable for users when they upgrade to Android 13.

Android 7.91 Release Summary

MaaS360 makes the Android app version 7.91 available on Play Store on 26 June 2022.

Defect	Summary
H-54886	When administrators published a policy with new passcode settings, the passcode evaluation failed on Samsung Device Admin (DA) devices.
H-54885	The MaaS360 for Android app crashed when users upgraded the MaaS360 app on activated devices.
C-44978	Some Device Owner (DO) devices that were enrolled through Knox Mobile Enrollment (KME) automatically signed off after the enrollment.

Android 7.90 Release Summary

MaaS360 makes the Android app version 7.90 beta available in Play Store on 6th June 2022.

Configure background apps for Android Kiosk mode >>

When a device is locked to single app or multi-app kiosk mode, you can specify a list of apps that are allowed to run in the background. These background apps are hidden from the Kiosk home screen and users cannot interact with them. Kiosk apps can invoke these background apps to execute custom system functions. For example, you can add Android System WebView as a background app to render web content on some Android devices.

Note: Supported only for Android Enterprise devices.

All MaaS360 apps are now compliant with Android 12 >>

MaaS360 is now fully compatible with Android 12 and adopts all the behavior changes related to Android 12.

Behavior changes

- **Special permission required to set exact alarms** - Exact alarms schedule an alarm to be delivered precisely at the stated time. MaaS360 uses exact alarms to perform time-sensitive actions such as Out of Compliance Timer, Calendar/Task reminders, and Selective Wipe on inactivity. Apps that target Android 12 must have the `SCHEDULE_EXACT_ALARM` permission in order to set exact alarms. The apps that have `SCHEDULE_EXACT_ALARM` permission can access **Alarms & reminders** capability that appears within the **Special app access** screen in system settings. This permission is auto-granted to apps on new enrollments or upgrade to MaaS360 app version 7.90. However, both users and system can revoke **Alarms & reminders** special app access. If the Alarms & Reminders access is revoked, the app stops functioning and all future exact alarms are cancelled.
- **Support for new Bluetooth permissions to use Bluetooth features** - Apps that target Android 12 must use the new dynamic permissions BLUETOOTH_SCAN, BLUETOOTH_ADVERTISE and BLUETOOTH_CONNECT to access Bluetooth functionality. To grant the new Bluetooth permissions, users must allow the app to access **Nearby devices**. This permission is not granted by default. Users must grant the **Nearby devices** permission on the device to allow the device to discover and connect to nearby Bluetooth devices. MaaS360 app needs this permission to collect peripheral device data.
- **Passcode length & Quality cannot be set for profile owners anymore** - In the previous releases, the passcode settings: Minimum Passcode Quality and Minimum Passcode Length were deprecated for Android 12+ Profile Owner (PO) devices in favor of Minimum Password Complexity, but administrators were allowed to push deprecated policies to the devices. The deprecated policy settings: Minimum Passcode Quality and Minimum Passcode Length are no longer supported on Profile Owner (PO) devices when they enroll with or upgrade to MaaS360 for Android app version 7.90+. Administrators must use Minimum Password Complexity to set passcode settings on PO devices running MaaS360 for Android app version 7.90+.

Control notification permission for managed apps through Security policies >>

Android 13 introduces a new runtime notification permission, allowing users to focus on the notifications that are most important to them. Apps that are installed on Android 13 will now request the notification permission from the user before posting notifications. Effective 10.86, MaaS360 makes it easier for administrators to control notification permission through Security policies. Administrators can use Android Enterprise policies to automatically grant notification permission to the managed Google Play apps, and also to block apps that use the notification permission on managed devices.

Note: Supported only for Android Enterprise devices.

Google Play app management enhancements >>

- **Granular instant installation options** - MaaS360 adds new granular instant installation options for Google Play apps - Install once and Retry installation. These options are available in the Add app workflow and the App Summary page. Instant once is the default option for the existing apps that have the Instant Installation option selected. Both the options install the app on devices automatically.
- **New granular installation state for the Install once option** - When an app is distributed with the Install once option, the Status is changed to **Distributed** and State is changed to **App Available with auto install once setting** in the App Distribution page.
- **Support for asynchronous API for better management of apps** - In the previous releases, MaaS360 used different synchronous APIs for various app management tasks, which caused issues in app config distribution and app distribution. Effective 10.86, MaaS360 moves to the newer Google API (asynchronous), wherein all those tasks are performed by a single API and thereby reducing the delays occurring across app config and app distributions.
- **Removed deep link support for app installation** - Users can no longer use deep links to install apps directly from the Play Store.

Added My Device section in Android Kiosk mode >>

MaaS360 adds the My Device section to allow users to view device related information such as Device ID directly in the kiosk mode. In previous releases, if MaaS360 app was not added to the kiosk launcher, users had to exit the kiosk mode and access the device related information from the MaaS360 app.

Defect Fixes

Defect #	Summary
44831	When a config file without an extension was pushed to internal device storage through Docs, MaaS360 automatically added a .unknown file extension. As a result, third-party apps were unable to read the file.
44788	Remote device enrollment via Experitest was unsuccessful, and a blank screen was displayed when the MaaS360 app was launched from the Work profile.
44704	The runtime permissions configured through Android MDM policies were not applied to the DO devices.
44702	Android device users did not receive email notifications for Exchange favorite contacts.
44506	Secure Mail attachments could not be opened/imported into a third-party app called Secure ID.
44296	The firewall policy settings are not applied to Samsung devices that are enrolled in Device Admin mode.
44277	After enrolling the Pixel 6 Pro device in Android Enterprise mode, the MaaS360 agent failed to report the Device Enrollment Mode information to the MaaS360 portal.
44244	Attachments in Outlook did not open with Secure Viewer on devices enrolled in DO mode.

Android 7.85 Release Summary

MaaS360 makes the Android app version 7.85 available on Play Store on 26 April 2022.

Defect Fixes

Defect	Summary
44635	When users tapped on a biometric lock setting on the device, an error message was displayed and the setting could not be modified.
44604	Duplicate entries were created for the same device on re-enrollment.
43878	Shared devices that were enrolled without a user displayed an error message when users tried to sign in to the MaaS360 app.

Android 7.81 Release Summary

MaaS360 makes the Android app version 7.81 available on Play Store on 23 March 2022.

Defect Fixes

Defect	Summary
H-54776	Fixed potential MaaS360 app crash on upgrading to the latest version.

Android 7.80 Release Summary

MaaS360 makes the Android app version 7.80 available on the Play Store on 17 March 2022.

New permission dialog for requesting location accuracy on Android 12 devices >>

On Android 12 or higher, users can specify the accuracy of the locations they share by choosing between Precise (`ACCESS_FINE_LOCATION`) or Approximate (`ACCESS_COARSE_LOCATION`) location accuracy.

When the MaaS360 app targets Android 12, the new system permissions dialog includes the following options for the user:

- **Precise**: Allows the MaaS360 app to get precise location information.
- **Approximate**: Allows the MaaS360 app to get only approximate location information.

Note: The Precise location pinpoints the device's location down to a few meters. MaaS360 uses this level of location accuracy to perform some of the crucial functions such as enabling geo-fencing, detecting insecure Wi-Fi connections, and recognizing the device's entry into preconfigured locations. MaaS360 Kiosk app requires this permission to display configured Wi-Fi networks and Bluetooth devices in close range.

Automatic generation of consistent device ID for Android 11 and lower devices >>

Google generates an enrollment-specific identifier for the device as a part of Android Enterprise enrollment. This identifier remains consistent even if the work profile is removed and enrolled again (to the same organization), or the device is factory reset and re-enrolled. To avoid a trial of duplicate device records, MaaS360 uses the same identifier for the device re-enrollment. In the previous releases, administrators had to enable this feature for Android 11 or lower devices through device enrollment settings. In this release, MaaS360 removes the parity between Android 11 and 12 versions and automatically enables this capability for all Android Enterprise devices.

End of support announcement

Android OS version 5 and 6 is no longer recommended by MaaS360

MaaS360 does not recommend running devices on Android versions 5 and 6. Effective October 2022, devices that run these OS versions will no longer receive new MaaS360 apps. For more information, see https://www.ibm.com/support/pages/node/6554444

Defect Fixes

Defect	Summary
44334	Devices that were activated in the SPS mode stopped reporting to the MaaS360 portal.
44327	When a user tried to change the From Date of a Calendar event, MaaS360 displayed a transparent background for the overlaid calendar, making it difficult for users to select a new date.
44304, 44171, 43888	Android devices did not receive the latest policy version from the MaaS360 portal.
44281	Android 12+ WPCO devices did not report IMEI to the MaaS360 portal.
44266	Proofpoint meeting URLs were not processed correctly in Secure Mail and meeting invites.
44211	Devices enrolled in bulk into the Device Admin mode unexpectedly rebooted shortly after enrollment and failed to retain kiosk settings after the reboot.
44117, 43833	The lock screen configuration settings are flagged as failed in the MaaS360 app > Settings > Corporate Settings.
44101	The Secure Mail app did not load inline images with the jpgx file extension.
44068	The Secure Mail app did not show emails that were sent from the Prowide app.
44049	Devices were flagged as non-compliant if the devices were not unlocked after a reboot.
44020	When administrators added some domains to the blocklist, other domains that were not specified in the blocklist were also blocked automatically.

Android 7.75 Release Summary

MaaS360 makes the Android app version 7.75 beta available on App Store on 10 February 2022.

Defect Fixes

Defect	Summary
43888, 44171, 44211	The default Android policy was incorrectly applied to the devices after the dynamic policy assignment.

End of support announcement

Android OS version 5 and 6 is no longer recommended by MaaS360

MaaS360 does not recommend running devices on Android versions 5 and 6. Effective October 2022, devices that run these OS versions will no longer receive new MaaS360 apps. For more information, see https://www.ibm.com/support/pages/node/6554444

macOS Release Summaries

macOS Release Summaries

macOS Agent 2.48.000, App Catalog 1.57.000, and macOS App Packager 1.47.000

MaaS360 makes the macOS Agent 2.48.000, App Catalog 1.57.000, and macOS App Packager 1.47.000 available on 27 September 2022.

Defect	Summary
44960	MaaS360 displayed an incorrect app installation status.

macOS Agent 2.47.000 Release Summary

MaaS360 makes macOS agent 2.47.000 version available on 24 June 2022.

- Minor fixes and improvements.

macOS Agent 2.46.000, App Catalog 1.56.000, and App Packager 1.46.000 Release Summary

MaaS360 makes macOS Agent 2.46.000, App Catalog 1.56.000, and macOS App Packager 1.46.000 available on 14 April 2022.

- Minor fixes and improvements.

macOS Agent 2.45.100, App Catalog 1.55.100, and macOS App Packager 1.45.000 Release Summary

MaaS360 makes macOS Agent 2.45.100, App Catalog 1.55.100, and macOS App Packager 1.45.000 available on 17 February 2022.

- MaaS360 Packager notarization is now compatible with Xcode 13.
- Minor fixes and improvements.

Defect Fixes

Defect	Summary
44326	The installation of the MaaS360 App Catalog app failed unless Rosetta was already installed.

Cloud Extender Release Summaries

MaaS360 Cloud Extender Release Summaries

Cloud Extender 3.00.001 Release Summary

The following features and fixes were fixed in this release:

- Deprecation of Windows 2012 support
  - Information about upgrading to Cloud Extender 3.x version

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.

Agent version: v3.00.001

Cloud Extender 2.106.700 Release Summary

The following features and fixes were fixed in this release:

New health check alerts for MEG for Apple WKWebview >>

New Enterprise VPN Gateway alerts evaluate the status of MEG and, if triggered, notify administrators by email message or text message about the following events:

- Relay server is not reachable
- DNS settings are invalid or corrupted
- Maximum limit reached for hosts that are not connected

From the MaaS360 Portal, administrators can choose remediation actions to troubleshoot the events.

Fix #	Description
45223	Modern Authentication failure when Azure account is on a GCC High environment.
45211	Cloud Extender cannot install latest MEG module.
45187	Email Notification not working after Modern Auth was enabled.
45160	Android device unable to connect to intranet resources post MEG module upgrade.
45111, 45080, 44461	MEG failure due to incorrect .net version.
44940	After upgrade, MEG was unable to connect.
44184	iOS devices failing to connect due to MEG module crash.

Agent version: v2.106.701.001

Features included in agent: new signing certificate

Cloud Extender 2.106.651 Release Summary

The following issues were fixed in this release:

Agent only : v2.106.651.002

#	**Description**
44447	Cloud Extender agent hanging. *note this was partially fixed in v2.106.600, but after reviewing logs additional scenarios were found that still had CE agent hanging.

Cloud Extender 2.106.650 Release Summary

The following security issues and fixes are included in this release:

Fixes

#	Description
45071	Cloud Extender EAS data sync errors when migrating to O365 and Modern Authentication

CVE Security Bulletins

The following CVE security bulletin was issued for this release: https://www.ibm.com/support/pages/node/6826107

Affected Product(s)	Version(s)	CVE(s)
IBM MaaS360 Cloud Extender Agent	2.106.600.007 and prior	CVE-2022-32205, CVE-2022-32206, CVE-2022-32207, CVE-2022-32208
IBM MaaS360 Cloud Extender Base	2.106.600 and prior	CVE-2022-32205, CVE-2022-32206, CVE-2022-32207, CVE-2022-32208

To Upgrade MEG/VPN Modules

- Cloud Extender agent v2.106.650.002 : IBM Documentation Page

Cloud Extender 2.106.600 Release Summary

The following security issues and fixes are included in this release:

- Upgrade of log4net

#	Description
43518	Auto Quarantine not approving specific devices.
44447	Cloud Extender agent hanging.
44448	LDAP Authentication failed when OU added.
44029	LDAP groups failing after adding Azure User Visibility.

CVE Security Bulletins

The following CVE security bulletin was issued for this release: https://www.ibm.com/support/pages/node/6826101

Affected Products(s)	Version(s)	CVE(s)
IBM MaaS360 Cloud Extender Agent	2.106.500.011 and prior	CVE-2022-27780, CVE-2022-27781, CVE-2022-27778, CVE-2022-27782, CVE-2022-30115, CVE-2022-27779, CVE-2022-27774, CVE-2022-27776
IBM MaaS360 Cloud Extender Base	2.106.500 and prior	CVE-2022-27780, CVE-2022-27781, CVE-2022-27778, CVE-2022-27782, CVE-2022-30115, CVE-2022-27779, CVE-2022-27774, CVE-2022-27776
IBM MaaS360 Configuration Utility	n/a	none
IBM MaaS360 Email Notification	n/a	none
IBM MaaS360 Exchange ActiveSync	n/a	none
IBM MaaS360 User Visibility LDAP	n/a	none
IBM MaaS360 User Authentication	n/a	none
IBM MaaS360 Mobile Enterprise Gateway	n/a	none
IBM MaaS360 Configuration Utility	n/a	none

To Upgrade Cloud Extender Agent and MEG/VPN Modules

- MEG/VPN: IBM Documentation Page
- Cloud Extender agent v2.106.600.007: IBM Documentation Page

Cloud Extender 2.106.500 Release Summary

The following features and fixes were fixed in this release:

Certificate request Prioritization for New Enrollments : with the 2.106.500.011 Cloud Extender agent and modules the MaaS360 platform will now detect new enrollment requests and delivery the certificate to these devices as priority allowing certificate delivery for new wifi, mail and vpn requests over existing enrolled devices.

Fix #	Description
44710	Certain intranet sites show blank or incomplete page shown when connected through proxy.
44285	Cloud Extender Visibility module not syncing users and groups.
44585	NTLM authentication failing when connecting through MEG

The following security issues were fixed in this release:

- https://www.ibm.com/support/pages/node/6592807
- https://www.ibm.com/support/pages/node/6592799

CVE Security Bulletins

The following CVE security bulletin was issued for this release:

Affected Product(s)	Version(s)	CVE(s)
IBM MaaS360 VPN Module	2.106.100 and prior	CVE-2022-0547, CVE-2022-0778
IBM MaaS360 Mobile Enterprise Gateway	2.106.200 and prior	CVE-2021-22060, CVE-2022-22965, CVE-2022-22950, CVE-2021-28165, CVE-2021-34429, CVE-2021-28164, CVE-2021-34428, CVE-2021-28163, CVE-2021-28169
IBM MaaS360 Cloud Extender Agent	2.106.100.008 and prior	CVE-2022-0778

To Upgrade Cloud Extender Agent and MEG/VPN Modules

- MEG/VPN: IBM Documentation Page
- Cloud Extender agent v2.106.500.011: IBM Documentation Page

Cloud Extender 2.106.400 Release Summary

The following security issues were fixed in this release:

CVE Security Bulletins

The following CVE security bulletin was issued for this release: https://www.ibm.com/support/pages/node/6578693

Affected Products and Versions

IBM MaaS360 Mobile Enterprise Gateway	2.106.200 and prior
IBM MaaS360 Configuration Utility	2.105.200 and prior

To Upgrade MEG/VPN Modules

- MEG/VPN: IBM Documentation Page

Cloud Extender 2.106.300 Release Summary

The following fixes were added in this release:

Fix #	Description
43943	Fix applied to display of the correct version of the MEG module within the UI.
44275	SCEP certificates failing to GETCACert
44149	Error when configuring Cloud Extender Office365 Integration

Cloud Extender 2.106.200 Release Summary

The following fixes were added in this release:

Fix #	Description
43396	Not able to access personal drive after password changed after changing AD password.
39818	No prompt for re-authorizing using Enterprise Gateway changing AD password.
42287	IBM Java upgrade to version 8.0.6.36.

Cloud Extender 2.106.100 Release Summary

The following security issues were fixed in this release:

CVE Security Bulletins

The following CVE security bulletin was issued for this release: https://www.ibm.com/support/pages/node/6549670

Affected Product(s)	Version(s)
IBM MaaS360 Base Module	2.105.300 and prior
IBM MaaS360 VPN Module	2.105.300 and prior
IBM MaaS360 Certificate Integration Module	2.105.300 and prior
IBM MaaS360 Cloud Extender Agent	2.105.300.005 and prior

To Upgrade Cloud Extender Agent and MEG/VPN Modules

- MEG/VPN: IBM Documentation Page
- Cloud Extender agent v2.106.100.008: IBM Documentation Page