10.84 Release Summary

iOS

New Extensible Single Sign-On policy setting for iOS devices >>

Administrators can use the new Extensible Single Sign-On policy setting to enable Single Sign-On for native apps and websites on managed iOS devices. This configuration is used by identity providers such as IBM Security Verify to implement seamless authentication when users sign in to native apps and websites. Users authenticate once and then gain access to subsequent native apps and websites automatically.

Activation of eSIMs for Apple devices through MaaS360 portal >>

MaaS360 adds a new dynamic device-level and group-level action **Manage eSIM Configuration** to allow administrators to remotely activate an eSIM for managed iOS devices. The configuration contains an eSIM URL that is purchased from vendors such as Verizon and AT&T. After the deployment, MaaS360 installs the eSIM configuration profile and then activates the cellular plan on iPad devices that support eSIM.

Consistent user interface for authentication screens >>

MaaS360 now displays a unified authentication screen across all platforms. In 10.84, MaaS360 extends the consistent authentication UI from Shared device login workflow to Forgot PIN, password-protected documents, and app sign-in workflows.

Note:

- Requires MaaS360 for iOS app version 4.80+.
- When the authentication mode is set to Corporate (Azure), users are redirected to the Azure portal for authentication during enrollment. For Azure enrollments, administrators should have the unified authentication feature enabled and the authentication via Azure AD allowed for MaaS360 to display the unified authentication screen.

macOS

Support for new group-level action to retrieve personal recovery key on previously encrypted devices >>

In 10.84, MaaS360 adds the group-level action **Escrow FileVault Recovery Key**, allowing administrators to retrieve the FileVault recovery key from previously encrypted devices. When devices are migrated from another UEM to MaaS360, administrators can easily create a smart group with devices that do not have a FileVault recovery key and then push the **Escrow FileVault Recovery Key** action to retrieve recovery keys from multiple devices at once. In the previous releases, administrators could retrieve the FileVault recovery key at an individual device level.

Enhancements to System Extensions macOS policy >>

MaaS360 adds new parameters to the System Extensions policy:

- **Allow All System Extensions**: If this setting is turned on, MaaS360 loads all the system extensions that are signed with the trusted/allowed Team identifier (developer). In the previous releases, administrators had to manually specify the bundle IDs of the system extensions that are allowed to load.
- **Removable System Extension Bundle IDs**: The comma-separated bundle IDs of the system extensions that are allowed to remove themselves from the machine.

Android

Restrict personal accounts in Google Play >>

MaaS360 adds an advanced Android Enterprise policy setting **Restrict Personal Accounts in Google Play**. When this setting is enabled, users can add personal Google accounts to use services like Maps, Mail, or Drive, but they cannot use personal Google accounts to install Google Play apps. **Note**: Applicable for both G Suite and non-G Suite accounts.

Check the status of devices registered to Azure AD on the MaaS360 for Android app >>

After registering the device to Azure AD for Conditional access, users can tap the new **Recheck Status** button to check the latest device registration status. If the authentication details are missing or the device is removed from the Azure portal, users are redirected to the authentication screen to complete the device registration again.

Password complexity enhancements >>

MaaS360 extends the password complexity policy setting from Profile Owner to Device Owner devices. The **password complexity feature** sets device-wide password requirements in the form of predefined complexity buckets (High, Medium, Low, and None). If the administrator defines the password complexity policy setting, then the older passcode policies (Minimum Passcode Quality, Minimum Passcode Length) are not respected. **Note**: Supported on Android 12+ Profile Owner and Device Owner devices. Requires Android App 7.50+ for PO. Requires Android App 7.70+ for DO.

Consistent Device Identifier for Android Enterprise enrollments >>

Google generates an enrollment-specific identifier for the device as a part of Android Enterprise enrollment. In the previous releases, a new identifier was generated whenever a device was enrolled, which left a trail of duplicate records when the same device was re-enrolled. Effective 10.84, a consistent device identifier is generated which remains the same for the device even if the work profile is removed and re-enrolled or the device is wiped and re-enrolled. Requires Android app 7.70+

Note:

- On Android 12+ devices, the consistent device ID is automatically generated for Android devices that are enrolled in Android Enterprise mode.
- On Android 11 and lower devices, administrators must set the custom enrollment attribute ***use_persistent_device_id*** to ***true*** to enable consistent device ID for Device Owner (DO) and Work Profile on Corporate Owned (WPCO) devices. For more information about enrollment attributes, see https://www.ibm.com/docs/en/maas360?topic=portal-additional-android-enterprise-enrollment-attributes

Work Profile enrollment flow changes >>

To generate a consistent device ID, MaaS360 introduces minor changes in the Work Profile enrollment flow. Effective 10.84, the authentication screen is displayed after the work profile creation.

- **Old flow** - EnrollmentInstrumentation > Authentication > WorkProfile Creation > Google Account Creation
- **New Flow** - EnrollmentInstrumentation > WorkProfile Creation > Authentication > Google Account Creation

Platform

Support viewing of future-dated subscriptions on MaaS360 portal >>

MaaS360 portal displays the future-dated subscriptions. On the start date of a future-dated subscription, the corresponding license bundles will turn active.

Support for multiple user authentication types and unified authentication >>

MaaS360 redesigns enrollment and authentication settings to support multiple user authentication types. MaaS360 agent apps (Windows, Android, iOS) now display consistent user authentication screens for various authentication workflows such as Shared device login and Forgot PIN.

In the redesigned Settings page,

- MaaS360 supports multiple authentication types for enrollment. Based on their user-level authentication type, users can authenticate against Azure AD, SAML, or Local. For example, administrators can have employees authenticate against Azure AD and contractors use Local credentials. In the previous releases, administrators could select only one authentication mode as default for all enrollments.
- Administrators can set an authentication type as default. The default authentication type is used in auto-provisioning, Add Device, and Add User workflows.
- MaaS360 displays configured user directories and authentication modes in a centralized location.

Note:

- Requires MaaS360 for iOS app 4.80+, MaaS360 for Android app 7.60+, and MaaS360 for Windows app 4.55+.
- These settings are available to new customers (enrolled after 10.84) by default and for the existing customers who have the Unified Sign-in enabled.
- Existing customers must reach out to the MaaS360 support team to get this feature enabled for their accounts.
- This feature will be rolled out to existing customers in phases in the future.

For more information on Directory and Enrollment settings, see https://www.ibm.com/docs/en/maas360?topic=portal-configuring-directory-enrollment-settings-in-maas360.

Additional control for showing blocked images from external domain emails >>

When the remote images from external domains are blocked by the administrator, the remote images in emails are automatically hidden. Effective 10.84, MaaS360 adds additional controls to allow users to view the images by tapping the banner at the top of the email when the remote images are blocked.

Certificate pinning enhancements >>

In the third phase of series of enhancements, MaaS360 adds support to enforce Certificate pinning on all devices or specific user or device groups. When Certificate pinning is enabled for specific groups and devices, the server's certificate is pinned to MaaS360 apps only after persona policies reach the device. Administrators can configure the certificate pinning for Email, Gateway, and workplace apps through Persona policies irrespective of whether certificate pinning is turned on or off.

App Management

New app update settings for Managed Google Play apps >>

MaaS360 adds granular auto-update settings for Managed Google Play apps. Administrators can configure the auto-update mode (Default, Postponed, and High Priority) to ensure that the devices receive the latest updates automatically and also control how the apps must be updated on the devices. **Note**: Supported only on Android Enterprise devices. Applicable only to Google Play apps and Private Apps for Android Enterprise. The app update settings are configured at the individual app level.

App configuration support for Chrome and Gmail apps >>

MaaS360 now allows the deployment of managed app configurations for Chrome and Gmail apps. With this support, administrators can easily push app configurations for Gmail and Chrome apps through App Configurations instead of MDM policies. **Note**: Requires MaaS360 for Android app version 7.60+.

Faster retry of app config redeployment on failure >>

MaaS360 now attempts to redeploy app configurations after a period of 5 minutes if the deployment of app configuration fails after the enrollment. In the previous releases, MaaS360 initiated a retry after a delay of 15 minutes.

Advanced app compliance policies to control user-installed apps on managed devices >>

MaaS360 extends the **Configure allowed apps** and **Configure restricted apps by permission** settings from Device Admin to Android Enterprise policies. Administrators can use these policies to remotely control (allow/block) user-installed apps on managed devices.

- **Configure allowed apps**: When administrators configure allowed apps, all other user-installed apps on the device are disabled.
- **Configure restricted apps by permission**: Administrators can specify permissions that are not allowed on the managed devices. The user-installed apps that use restricted permissions are disabled until those permissions are revoked by the users from the device settings.

Note: These settings are not applicable to system apps, first-party apps, and apps installed via the App catalog.

Windows

Windows 10+ device bulk enrollment support for unified authentication >>

MaaS360 provides a new feature that allows end users to authenticate (by providing their corporate credentials) against MaaS360, AD/LDAP, Azure, or an identity provider (Okta, PingIdentity, Azure, other third-party providers) to enroll Windows 10+ devices into MaaS360. End users are prompted to provide their credentials to authenticate before bulk enrolling their devices. If the end user dismisses the prompt, they are prompted again in an hour to authenticate against their corporate credentials before the MDM profile is added to the device.

Webservices

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

- The Get Audit of Policy Changes API has been introduced to fetch audits of all the policy changes made to a billing ID of an organization.
- The Add User API has been enhanced to support authType parameter to enable customers to pass any of the configured auth types in the API.
- MaaS360 adds new parameters instantUpdate and autoUpdateMode to addPlayApp API to configure automatic updates and select the default automatic update mode for Google Play apps.

For more information, see the latest Webservices guide.

10.83 Release Summary

iOS

Advanced iOS 15 restrictions >>

MaaS360 adds advanced policy settings for iOS 15 devices:

- Force On Device only Translation: When this setting is turned on, the Translate app does not send any content to the Siri servers for the purposes of translation. The default value is False. Supported on iOS 15 and later.
- Allow iCloud Private Relay: When this setting is turned off, the Private Relay option under iCloud+ is unavailable. **Note**: Supported only on iOS 15+ Supervised devices.
- Allow Pasteboard content between managed and unmanaged apps: When this setting is turned off, restricts copy and paste between managed and unmanaged apps through pasteboard. If this setting is turned on, copy and paste functionality respects **Allow Open from Managed to Unmanaged Apps** and **Allow Open from Unmanaged to Managed Apps**.
  Example scenario:

Allow Open from Managed to Unmanaged Apps = False	Allow Open from Unmanaged to Managed Apps = True	Allow Pasteboard content between managed and unmanaged apps = True
Managed documents cannot be opened with unmanaged apps.	Unmanaged documents can be opened with managed apps.	The data that is copied from managed apps cannot be pasted in unmanaged apps. The data that is copied from unmanaged apps can be pasted in managed apps.

iOS 15 same-day support >>

MaaS360 announces same-day support for iOS 15. With this support, new iOS 15 devices enroll with MaaS360, and existing devices upgrading to iOS 15 continue to work seamlessly without any disruption.

macOS

Advanced macOS 12 policies >>

MaaS360 adds two new policy settings for macOS 12 devices:

- Allow erase all content and settings: The **Erase All Content and Settings** option in **Settings** > **General** > **Reset** is used to erase all settings, media, and data on macOS devices. When this setting is turned off, the **Erase All Content And Settings** option in the Reset UI is unavailable. Supported on macOS 12 and later. The default value is True.
- Allow non-admin user to approve kernel extensions: In the previous releases, only admin users could approve kernel extensions that are not explicitly allowed by configuration profiles. When this setting is turned on, non-admin users can approve additional kernel extensions in the Security & Privacy preferences. Supported on macOS 11 and later. The default value is False.

Certificate pinning support for macOS >>

MaaS360 now extends cert pinning support to macOS devices. With this support, the MaaS360 app validates the server certificate as a part of communication to MaaS360 servers, including enrollment. If an insecure network connection or proxy is detected on the device, MaaS360 displays the Untrusted connection error message and then terminates the enrollment or stops the apps such as MacOS agent, App Catalog, or App Packager from functioning.

Note: Customers must reach out to the MaaS360 Support team for enabling the new cert pinning feature. Requires macOS agent app version 2.43.100, App Catalog version 1.54.000, and App Packager version 1.44.000.

macOS 12 Monterey same-day support >>

MaaS360 announces same-day support for macOS 12 Monterey. With this support, new macOS 12 devices enroll with MaaS360, and existing devices upgrading to macOS 12 continue to work seamlessly without any disruption.

Android

ZT-iFrame for Google Devices >>

MaaS360 embeds the zero-touch iframe in the MaaS360 portal. The zero-touch iframe allows administrators to configure zero-touch enabled devices with a device policy controller (DPC) directly from within the MaaS360 portal. In the previous releases, administrators had to download the DPC configuration (JSON file) and then manually apply the configuration through the zero-touch portal. With iframe, administrators can link their zero-touch accounts with MaaS360 Portal. As part of this process, administrators create a default zero-touch configuration profile that is automatically applied to devices without a configuration. **Note**: Administrators can continue to use the zero-touch portal to upload and modify configuration profiles.

Fixed background location access notifications issue >>

During the Android Enterprise (DO and PO) enrollment, the MaaS360 for Android app granted itself Location permission in the background without allowing users to modify the permission from the device Settings. Effective OS version 11, Android started displaying periodic notifications to remind the users that the MaaS360 app has access to their location. To avoid the background location access reminders, MaaS360 now allows administrators to configure runtime permissions in a way that the Location permissions are controlled by the end-users. MaaS360 adds a new policy setting to mark devices as non-compliant if the MaaS360 app does not have location permission.

Enhancements to Android Enterprise runtime permissions >>

MaaS360 now allows administrators to control how Location, Storage, and Phone permissions are granted to the apps. In the previous releases, those permissions were auto-granted during the enrollment. MaaS360 removes the unsupported permissions, adds support to grant all permissions at once, and more.

Deprecation of Samsung Knox License (SKL) policy >>

Samsung makes premium Knox Platform for Enterprise (KPE) licenses available to all customers at no cost. See the announcement here: https://www.samsungknox.com/en/blog/knox-platform-for-enterprise-free-for-customers. In previous releases, customers had to purchase the premium Knox Platform for Enterprise (KPE) licenses and activate those licenses through security policies in the MaaS360 portal. Effective 10.83, MaaS360 removes the policy setting **Samsung Knox License (SKL)** from the MDM policies. **Path**: Android MDM policies > **OEM Settings** > **Samsung License Management** > **Samsung Knox License (SKL)**

Note: This change will be implemented as a part of DD after the 10.83 release. Customers who have already activated KPE Premium licenses through the MaaS360 Security policies must upgrade to the MaaS360 for Android app version 7.55 or later to avoid unexpected issues that might lead to re-enrollment of devices or license expiration error messages.

Trusteer Threat Management enhancements >>

MaaS360 includes new trigger events for the quicker detection of risk items on devices such as Root status change, Insecure Wifi detection, Malware detection, and so on. Effective 10.83, MaaS360 uploads the scan results to the MaaS360 portal in near real-time. In the previous releases, it took about 20 minutes for MaaS360 to upload the latest scan data to the MaaS360 portal. In addition to that, MaaS360 adds support for automatic uninstallation of the apps on Device Owner devices if the malware is detected.

Improvements to zero-touch JSON file size and download speed >>

MaaS360 improves the zero-touch JSON file download speed and removes the file size restriction of 2 KB.

Validation for Factory Reset Protection (FRP) policy setting >>

The Factory reset protection (FRP) policy setting determines which users can unlock a device that is reset to factory settings. When the administrators enable FRP, they must provide at least one Google User ID in the policy setting: **Authorized accounts to override**. If this prerequisite is not met, a validation message is displayed when publishing the policy. To know more about FRP in MaaS360, see Factory reset protection. **Note**: The existing policies that have the FRP policy enabled and the setting: **Authorized accounts to override** left blank will display an error message when those policies are published.

Disable Factory Reset Protection (FRP) when issuing device wipe action >>

Factory Reset Protection (FRP) is automatically activated on Device Owner (DO) and Work Profile on Corporate Owned (WPCO) devices after the device wipe. Effective 10.83, when issuing the wipe action, administrators can select **Remove Factory Reset Protection** to disable activation of FRP on DO and WPCO devices. When this option is selected, users can unlock the device without the Google Account verification and start using the device after the device wipe. **Note**: The **Remove Factory Reset Protection** option is displayed on the Wipe action workflow regardless of whether the FRP policy is enabled or not. In the previous releases, this option was displayed only when the FRP policy was enabled.

Android 12 Zero-day support >>

When MaaS360 runs on Android 12, there will be behavior changes that impact some of the features in the MaaS360 app. MaaS360 first-party apps and SDK apps will continue to work on Android 12.

Removed Samsung Keyboard options from App Compliance policies >>

MaaS360 removes the Samsung keyboard settings from security policies to prevent administrators from disabling the native Samsung keyboard on the devices. Samsung includes the native keyboard on the devices by default. Administrators did not have to enable them through policies. But when the keyboard settings were disabled through policies, the native keyboard was completely blocked on the devices. Effective 10.83, the following policy settings are unavailable in the MaaS360 portal:

- MDM policies > **Android Enterprise Settings** > **App Compliance** > **Samsung Keyboard (OneUI 2.0)** and **Samsung Keyboard (OneUI 2.1)**

New custom command to remotely clear app data >>

In the previous releases, MaaS360 added custom command support, allowing administrators to execute remote actions on the managed Android devices. In this release, MaaS360 adds a new command to allow administrators to remotely clear the app data. **Syntax**: clear-app-data <comma-separated app IDs>. **Example**: *clear-app-data com.ibm.security.verifyapp, com.ibm.gts.banorte.epass*. **Note**: Requires MaaS360 for Android app version 7.60 or later. Supported only on Android Enterprise devices running OS version 9 or later. The action fails if the target apps are not installed on the device.

Removed ActiveSync support for Motorola email client >>

MaaS360 removes Motorola email client support from the Device Admin ActiveSync policies. As a result, administrators can no longer use Device Admin policies to configure ActiveSync on the Motorola email client.

Strict scheduler for device payloads >>

MaaS360 extends strict scheduler support from device heartbeat to payloads. With this support, MaaS360 uploads payloads in real-time. When this policy is turned on, the payloads upload timer strictly follows the value defined in the Data Collection Frequency policy setting.

Refactored code to stop requesting permissions during the Bulk Enrollment >>

In the previous releases, MaaS360 allowed customers to enable the MaaS360 app to request permissions during the enrollment process. Effective 10.83, the MaaS360 app requests all the required permissions at the runtime for Device Admin Bulk Enrollments.

Minor UX changes to the Remove Work Profile action in the MaaS360 portal >>

MaaS360 renames the device-level acton **Remove Work Profile** to **Remove Control** in an effort to provide a consistent user experience across all Android Enterprise modes of operation - DO, PO, and WPCO. For WPCO devices, the default device wipe mode selection on the Remove Control window is changed from **Wipe all data** to **Wipe work profile only**.

AAPT2 enabled by default for Android app wrapping >>

In the previous releases, administrators had to use app wrapping parameters to enable AAPT2. Effective 10.83, AAPT2 is enabled by default for Android app wrapping. **Note**: Customers can continue to use the app wrapping parameters to set enableAAPT2 to false.

Platform

Downloading device agent logs from the MaaS360 Portal >>

Portal or partner administrators with master administrator status can now download device logs from the MaaS360 Portal that are uploaded to IBM Cloud without having to contact IBM Support to access these logs.

Note: This feature is only available to administrators or partner administrators with the Send Logs Mode access right that is assigned by default to the Service Administrator role.

MaaS360 audit data reports >>

To provide audit data for various reports, logs, and user interfaces that are available within the MaaS360 administration portal, the MaaS360 audit data reports offer a summary of audit logs. Currently, the audit logs are available for enrollments, devices, users, portal administration, policies, rules, settings, and services actions in the MaaS360 portal.

Cert pinning enhancements >>

Cert pinning can now be directly enabled at the customer level through the MaaS360 portal Settings page. MaaS360 adds the new **Validate Server Certificate** setting on the Settings page. Path: Setup > Settings > Device Enrollment Settings > Advanced > Validate Server Certificate. In the previous release, administrators had to contact support to get the cert pinning feature enabled for their accounts.

The MaaS360 app validates the server certificate as a part of communication to MaaS360 servers, including enrollment. If an insecure network connection or proxy is detected, MaaS360 displays an error message and then terminates the enrollment process.
Note: The enrollment/activation is terminated when an untrusted connection or proxy is detected on the device even if Certificate pinning is turned off.

Analytics

Enhancements to the User Risk Management feature >>

The Security Management feature comprises the Security Dashboard and Risk Rule Configurator. In 10.83, the feature offers the following enhancements that allow administrators to use the security dashboard and manage risk rules that apply to the MaaS360 customer account.

- **Risky users list**: Previously, for a user account, that is under risk and if that user is removed from MaaS360, then, a hyphen was displayed instead of the user name in the 'risky users' list. To effectively show which user account is at risk, the security dashboard now shows user names for such deleted user accounts instead of a hyphen in the 'risky users' list. However, user details such as email, user source, domain, user groups values are shown as hyphens for these user accounts as user details are not available in the MaaS360. On the next security dashboard refresh cycle, user accounts that are deleted in MaaS360 are no more shown in this user list.
- **Administrator actions on the Risk Rule Configurator** : In the Risk Rule Configurator, administrators can enable or disable a risk rule for the organization from the predefined risk rules. By default, every risk rule in the ruleset is enabled and severity is associated with each risk rule. With the 10.83 release, the administrator not only can enable or disable a risk rule but can also enable or disable a rule description under a risk rule. This capability provides more flexibility for administrators to use only those risk rule descriptions that are necessary for monitoring an organization's risk factors. This option to enable or disable any rule descriptions under a rule name is available for all risk rules in the ruleset. Example: Administrator can enable the **Older version of MaaS360 app** risk rule and choose to monitor only MaaS360 app version =7.30 AND Platform=Android and can enable this rule description and disable other rule descriptions under this rule name.

Apps

New OEM and App configuration >>

MaaS360 makes App Configuration and Android OEMConfig features that support multiple configurations per app available for all customers. This new OEM/App Configuration provides an enhanced administrator experience while configuring and managing them.

OEMConfig -

Administrators can use Android OEMConfig to remotely deploy OEM-specific settings to the managed devices. OEMConfig is an Android standard that allows device manufacturers to create custom OEM-specific settings for Android Enterprise devices. MaaS360 uses OEMConfig apps built by device manufacturers to deploy advanced device configuration settings that are not natively available in the MaaS360 portal. For example, you can use Samsung's Knox Service Plugin app to configure Knox security settings such as advanced VPN configurations on the device. The OEM apps use the managed app configuration to remotely configure those settings on the devices.

App Config -

Administrators can use app configurations to remotely push configuration settings for managed apps. App developers define managed app configurations and program the app to deploy remote settings. Administrators use these managed configurations to remotely push configuration settings for the apps. App configurations are deployed with the managed apps when the apps are distributed through the App Catalog. MaaS360 allows administrators to add multiple app configurations for an app so that each configuration can be distributed to different groups or devices. App configuration is supported for iOS apps, Google Play apps, and Private apps for Android Enterprise.

App Configuration support for Enterprise apps for Android >>

Effective 10.83, MaaS360 extends app configuration support to Enterprise apps for Android. In the previous releases, app configuration was supported for Google Play apps and Private apps for Android Enterprise. **Note**: Requires MaaS360 for Android app version 7.60+.

Windows

MDM enrollment support for Windows 10 Home devices >>

MaaS360 now allows users to enroll their Windows 10 Home devices into the MaaS360 Portal in MDM mode.

Previously, Windows 10 Home devices could not be managed by MaaS360 like other Windows 10 editions due to limitations from Microsoft. Also, the MDM agent did not support the installation of the MaaS360 MES agent automatically on Windows 10 Home editions.

With this release, MaaS360 provides a new section (unified enrollment configuration) in the branding workflow that allows administrators to set up user enrollment settings for Windows 10 Home devices. Before administrators can send out enrollment requests to users, administrators must first set up user enrollment settings for the Windows 10 Home setup page that is explained in Branding settings for Windows devices. The following scenarios are available in the branding settings to administrators for user enrollment settings:

- provide no setup link and no additional instructions in the branding settings
- provide only a setup link in the branding settings
- provide only additional instructions in the branding settings
- provide a setup link and additional instructions in the branding settings

After user enrollment settings are configured, administrators perform the following actions:

- generate the SelfExtractingOA.exe file (see the procedure in Configuring the Windows 10 Bulk Provisioning Tool configuration wizard to create a bulk provisioning tool executable)

- upload the generated SelfExtractingOA.exe file
- provide additional information to users on the Windows 10 Home enrollment landing page
- require users to accept the EULA before they can enroll devices

Device users can follow the steps at Enrolling your Windows 10 Home device (MDM) to enroll their Windows 10 Home devices in MDM mode.

Webservices

In this release, the Authentication 2.0 Web service API was updated to include authentication token validation error scenarios that pertain to HTTPS status code 401. The new response structure for any authentication token validation-related errors scenarios is covered in this web service API. For more information, see the latest Webservices guide.

What's New Since 10.83 Release Summary

Version 10.83.cd.20102021 Released 20 October 2021

Pass IMEI number to Device Owner devices through App Configurations >>

MaaS360 includes the new custom attribute %imei% in the App Configuration and Android OEMConfig workflows. Administrators can use this custom attribute to feed IMEI numbers to the managed apps and devices. When the configuration is distributed to a device, MaaS360 replaces this attribute with the IMEI number of that device.

In addition to the user-defined custom attributes, MaaS360 supports the following user and device attributes:

- %upn%
- %user%
- %username%
- %email%
- %domain%
- %deviceid%
- %imei%

Note:

- Supported only for Device Owner devices. MaaS360 does not collect IMEI numbers from Profile Owner and Work Profile on Company Owned (WPCO) devices.
- MaaS360 overrides existing custom attributes defined by the administrators with similar syntax.
- The custom attributes are case-sensitive.

10.82 Release Summary

iOS

Advanced iOS 14.5 restrictions >>

- Allow Auto unlock - Default value is true. When set to false, prevents users from unlocking their paired iPhone running iOS 14.5 with their Apple Watch. By default, users can use their Apple Watch to unlock their devices when a mask prevents Face ID from recognizing the face.
- Allow Unpaired External Boot Recovery - Default value is false. When set to true, allows users to boot iOS or iPadOS devices into Recovery Mode from an external host computer (unpaired host). By default, an external host computer cannot start a device in Recovery Mode. Note: Requires supervised devices running 14.5 or later.
- Force on Device only Dictation - Default value is false. When set to true, prevents the use of Siri for dictation. By default, users can use dictation to enter text with many apps and features that use the keyboard on the devices.

Android

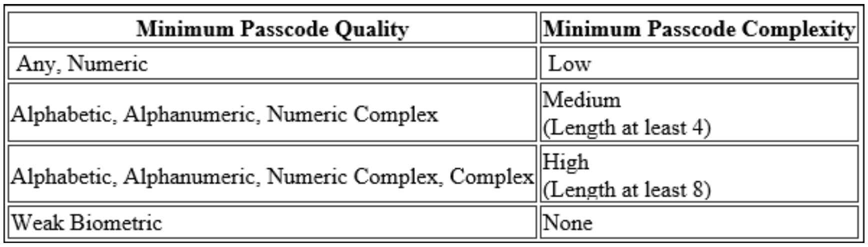
Enhanced SafetyNet attestation to comply with the Android compatibility guidelines >>

In the previous releases, MaaS360 implemented SafetyNet Attestation API, an anti-abuse API that validates whether the device the MaaS360 for Android app is installed on satisfies the Android compatibility tests. By default, a stricter verdict of device integrity was enabled in the background (the attestation strictness was set to High). In this release, as per the guidelines and requirements of Google, MaaS360 adds a new device enrollment setting **Attestation Strictness** that allows administrators to set the device attestation strictness to High or Moderate. When set to **High**, MaaS360 evaluates whether the device passed Android compatibility tests required to be qualified as a Google-certified Android device. When set to **Moderate**, MaaS360 checks whether the device is tampered with or compromised without performing any Android compatibility tests. For example, rooted devices will fail this test.

Administrators can enable hardware-based attestation to enable the use of hardware-based security features (e.g. hardware-backed key attestation) to influence the evaluation for device compatibility.

Passcode policy changes for Work Profile on Android 12 or later >>

Effective Android 12, Profile Owner (PO) devices require a passcode to be set in terms of complexity. MaaS360 adds a new policy setting **Minimum Passcode Complexity** that can be used to set device-wide and Work profile password restrictions in the form of predefined complexity buckets (High, Medium, Low, and None). When the devices upgrade to Android 12, a new **Minimum Passcode Complexity** setting will be applied to the devices based on the existing **Minimum Passcode Quality** setting configured in the portal.



Minimum Passcode Quality	Minimum Passcode Complexity
Any, Numeric	Low
Alphabetic, Alphanumeric, Numeric Complex	Medium (Length at least 4)
Alphabetic, Alphanumeric, Numeric Complex, Complex	High (Length at least 8)
Weak Biometric	None

Note: The default value is **Low**. Administrators can continue to use the Minimum Passcode Quality policy setting to apply password restrictions to the Android Profile Owner devices 11 or earlier.

Additional behavior changes when MaaS360 targets Android 11 APIs >>

In the second phase of the series of enhancements, when MaaS360 targets Android 11 APIs on MaaS360 for Android app 7.50, there will be an impact on the Device Admin bulk enrollment and docs distribution features and changes for Files, Media, and Location permissions. **Note**: Requires MaaS360 for Android app 7.50 or later.

New restriction to control location services on Android 11+ Device Owner devices >>

MaaS360 adds a new policy **Enable Location on device** to allow administrators to remotely control location services on Android Enterprise devices. However, users can manually turn the location service On or Off from the location settings after the policy is applied. **Note**: Requires MaaS360 for Android app 7.50 or later. Applicable only to Android 11+ devices that are enrolled in Device Owner mode. The default value is **Don't Set**.

Open .EML and .MSG files in the MaaS360 SDK app with the Secure Mail app >>

MaaS360 SDK apps will now support two new file formats: .EML and .MSG, allowing the users to open .MSG and .EML files with the Secure Mail app.

Support to sync Security & Compliance payload without delays >>

When there is a change in the compliance state of a device, MaaS360 will now instantly sync the compliance-related attributes in Security & Compliance payload without delays. This will expedite the process of detection of threats and enforcement of remediate actions.

New app wrapping config parameters >>

Administrators can use the new app wrapping config parameters: **enableAAPT2** and **coreLibraryRequired** to avoid compilation failures.

- **enableAAPT2** - If apps are built with AAPT2, the latest resource packaging tool, app compilation will fail during wrapping, and the `Wrapping Failure: Error in recompiling the app` error message is displayed. To avoid compilation failures related to AAPT, the enableAAPT2 parameter must be set to `true`.
- **coreLibraryRequired** - When developing the app, if the `additionalParameters =["--core-library"]` library is used in dexOptions in the build.gradle file, app compilation will fail and an error message is displayed. To avoid a compilation failure during app wrapping, the coreLibraryRequired parameter must be set to `true`.

macOS

FileVault disk encryption on a macOS device that was previously encrypted by a device user >>

In the previous releases, the FileVault recovery keys could be escrowed only from the managed devices that have the FileVault disk encryption enabled through MaaS360 policies. In this release, MaaS360 adds support to retrieve the recovery keys from the macOS devices that were already encrypted by the users or if the devices are being migrated from another UEM to MaaS360 with FileVault enabled before the enrollment.

Deploy macOS System Extensions through security policies >>

Administrators can now use System Extensions to remotely install app extensions that extend the functionality of the operating system without requiring kernel-level access. The System Extensions are executed in the user space rather than Kernal space without compromising the security and stability of macOS. Even though System and Kernal extensions serve the same purpose, the System Extensions framework offers advanced security and reliability and can execute the tasks that were previously reserved for Kernal Extensions. After the installation, the System Extensions are available for all the users in the System and can be deleted by deleting the app. In the previous releases, users had to deploy System Extensions to the macOS devices through configuration files.

New settings to control System Preferences panes >>

MaaS360 adds new policy settings to allow administrators to remotely control new System Preferences panes: Apple ID, Sidecar, Family Sharing, and Classroom.

Platform

Search for devices with secondary mailbox configured by using Advanced Search >>

In this release, the new search category 'Mailbox Information' is added in the Advanced Search condition. For this search condition, the attribute 'Secondary Mailbox Present' is supported. Using this search condition and attribute, the administrator can search for devices that have a secondary mailbox configured. This search condition alongside search criteria such as Equal To, Is Empty, Is Not Empty, and Not Equal To, the administrator can search for more specific device results with secondary mailbox configured, not configured, is empty, or not empty values.

Enhancements to the certificate pinning feature >>

Certificate pinning is a security technique that is designed to secure the communications between the client app and the server from man-in-the-middle (MITM) attacks. With certificate pinning, any attempts to establish a connection by a server to a client app with untrusted certificates will be terminated. Effective 10.82, certificate pinning will be enabled at the customer level through the MaaS360 portal Settings page. In the previous releases, it was enabled through Persona policies and applied to the devices via groups. The MaaS360 app validates the server certificate as a part of communication to MaaS360 servers, including enrollment. If an insecure network connection is detected, MaaS360 displays the Untrusted connection error message and then terminates the enrollment process. **Note**: Customers must reach out to the MaaS360 Support team for enabling the new cert pinning feature. After enabling, administrators can view the new **Validate Server Certificate** setting in the Setup > Settings > Device Enrollment Settings > Advanced > Validate Server Certificate. However, administrators cannot control (enable or disable) this setting in this release.

License Management feature availability>>

MaaS360 offers a License Management feature by using which administrator can manage MaaS360 license parts for a customer account. The feature is available for new customer accounts and trial customers with device-based licenses that are signing up from IBM Marketplace or third-party marketplace. Existing customer accounts can contact the IBM MaaS360 Support team to enable this feature.

The feature offers greater control for administrators to assign licenses to a device, bulk assign licenses, monitor license usage, view license assignment, and bulk license assignment history reports. Additionally, administrators can use license settings to configure the overage settings, default licenses under base license, and add-on licenses during self-enrollment, self-activation, and bulk license assign actions.

Redesigning the guided tour experience for first time login to the MaaS360 customer account >>

MaaS360 offers a meaningful onboarding experience for administrators by providing guided tours on the first login to the MaaS360 portal customer account. With the click of 'Let's go' in the pop-up screen, the QuickStart walkthrough starts that guides administrators to review and complete the essential steps to enroll, manage, and secure devices. For customer accounts that have completed the quick start configuration, the guided tour starts at the MaaS360 Home page screen. This tour guides through some of the portal Home page essential functions such as Main Menu, My Alert Center, My Activity Feed, Quick Actions, Insights Advisor and Get Help. The walkthrough currently is offered in the English language. Hence, the previously shown welcome screen pop-up is displayed as a quick walkthrough for customer accounts that use the portal in other supported languages except for English.

App management

Enhancements to the App configuration feature >>

Administrators can use app configurations to remotely push configuration settings for the managed apps. These configurations are deployed with the managed apps when they are distributed from the App Catalog. MaaS360 now allows administrators to view and manage app configurations for all the platforms in the Apps > App Configurations page. Administrators can add multiple app configurations for an app so that the configurations can be distributed to different groups/devices. In the previous releases, administrators could create only one app configuration per app.

An app configuration can also be set as default. The default configuration will be pushed to devices if other configurations are not specified to the devices via group-based or device-based distribution. For example, consider a scenario wherein an administrator has defined multiple configurations C1, C2, C3 for the Microsoft Outlook app and distributed C1 to the G1 group, C2 to the G2 group, and set C3 as default. When the Microsoft Outlook app is distributed to G1, G2, and G3 groups, the devices in G3, which are not part of G1 and G2 will receive the default configuration C3. In 10.82, all the existing app configurations will be migrated to the new workflow and all the app configurations will be automatically marked as default. However, administrators can clear this setting from the app configuration detail view.

Analytics

New rule sets-Antivirus inactive and critical security patch missing are added in Risk Rule Configurator >>

The User Risk Management feature supports 2 more new rule sets in addition to the existing predefined rule sets in the Risk Rule Configurator. Administrators can choose to enable or disable evaluating devices under these rulesets and also configure the severity of the risk rules in the Risk Rule Configurator. These 2 rule sets are applicable on Windows devices only.

Antivirus inactive: If enabled, this rule checks for the inactive status of antivirus software that is installed on the Windows device. A Windows device might have one or more antivirus software that is installed on the device. If all the antiviruses that are installed on the device are inactive, then, the risk rule condition is met and a risk incident is created with default severity as 'High'. If at least one of the installed antivirus software is active, then, the risk score and risk incident that is associated with this risk rule are immediately removed from the security dashboard. Devices with no anti-virus installed are not evaluated under this risk rule.

Critical security patch missing: If enabled, the rule checks if a critical security patch is missing on the Windows device. The higher the number of critical security patches that are missing on the device, the higher the risk score and severity. The defined severity is based on 1 - 2 security patches missing, 3 - 5 security patches missing, or more than five security patches missing on the Windows device.

Improved flexibility for administrators to enable or disable individual rules under the rule sets >>

The Risk Rule Configurator offers predefines rulesets using which administrators can customize the risk model by enabling and disabling risk incidents according to their organization's needs. By default, all rule sets are enabled in the Risk Rule Configurator. With this release, these rule sets come along with an option to enable or disable individual rules under every rule sets. For example, the administrator can enable the ruleset "Device encryption" and still choose to enable only the "no encryption" rule name and disable the "Partial encryption" rule name. In this case, only devices with no encryption are evaluated for risk, and devices with partial encryption are not evaluated.

Administrators can also disable a rule name anytime that was previously enabled. In this case, risk incidents that are created when the rule name is enabled continue to show in the security dashboard and contribute to the risk score until the retention period for the risk incident is complete (60 days). In some cases, the risk score is adjusted to the risk incident created under the enabled rule name wherever applicable.

Webservices

In this release, MaaS360 updated Get User and Device Groups API that MaaS360 defined groups are available only if there are active distributions. In the Download Windows Dependency API, a new error message DEPENDENCY_NOT_PRESENT is added for 200 response code if a dependency is not present. For more information, refer to the latest Webservices guide.

10.81 Release Summary

iOS

Advanced restrictions for iOS 14 devices >>

MaaS360 adds a new policy setting **Allow Apple Personalized Advertisements** to allow administrators to restrict the use of users' data by the Apple advertising platform to deliver personalized ads on iOS 14 devices. This setting replaces **Limit Ad Tracking**, which will now be supported only on iOS 13 or lower versions. Administrators can now use the new policy setting **Preview Type** to control how the notifications previews should be displayed on the device. MaaS360 also adds a new supervised setting **Allow Near Field Communication** to allow administrators to restrict the use of NFC on iOS devices.

MaaS360 stops showing available iOS updates for non-supervised devices >>

MaaS360 no longer syncs the available iOS updates from Apple for non-supervised devices. For the supervised devices, MaaS360 will continue to display the available iOS updates in device summary > Hardware & OS > Available Updates.

Locate a device that is marked as lost >>

In 10.80, MaaS360 added separate APIs to mark devices as lost and mark devices as found. In this release, MaaS360 added a new API to locate the devices that are marked as lost. For more information, refer to the latest Webservices guide.

Android

Custom command support >>

Administrators can now issue custom commands to execute remote actions on the managed Android devices. After the specified action is executed on the device, the execution status can be tracked in the device history. **Note**: Requires MaaS360 for Android app version 7.40 or later.

Device admin deprecation >>

Google announced the deprecation of the legacy Device Admin (DA) for enterprise use effective with the Android 10 Q release. In an attempt to promote the adoption of Android Enterprise, Google deprecated Device Admin management capabilities over the past few releases. Effective 10.81, MaaS360 no longer supports Device Admin enrollments for new customers. For the existing customers who have been using DA, MaaS360® recommends that they adopt Android Enterprise. Customers who have BYOD program can use the migration option in the MaaS360 portal to move to Android Enterprise Profile Owner (PO) mode. Customers who want to move to Device Owner (DO) or Work Profile on Corporate Owned (WPCO) device modes, will require device factory reset to move.

Granular status and error reporting for apps marked for instant install >>

MaaS360 makes it easier for the administrators to troubleshoot issues with instant install apps by adding new granular app installation statuses and retry logic. With this support, the instant install apps will report accurate app failure status (Failed instead of Pending) and device state (Out of Compliance or Selective Wipe). The status can be tracked in real-time and in case of installation/upgrade failure, MaaS360 automatically retries app installation up to 3 times on OEM devices. **Note**: Requires MaaS360 for Android app 7.40. Supported on both Device Admin and Android Enterprise devices.

Work Profile on Corporate Owned (WPCO) enhancements >>

In the previous releases, MaaS360 added support for *Work Profile on Corporate Owned (WPCO),* the new Android Enterprise management scenario that offers strict separation between work and personal profiles on corporate-owned devices. Effective 10.81, in addition to QR code enrollment, MaaS360 adds Zero-Touch enrollment option to set up a work profile on company-owned devices and extends WPCO support to the Samsung devices. Administrators can also enforce a new restriction **Configure personal apps to be Blocked/Allowed** to allow/block the installation of specific apps via Google Play Store in the personal profile of a company-owned device.

Behavior changes when MaaS360 targets Android 11 >>

When the MaaS360 for Android app targets Android 11 APIs, MaaS360 can no longer access the entire external storage directories on the device. The access is limited to specific directories and specific types of media that is supported by those directories. This means that administrators can distribute files only to the selected directories through the MaaS360 portal. While importing files into Docs and PIM apps, MaaS360 no longer displays the custom File Explorer option. However, users can use the system Files option that provides similar functionality as custom File Explorer. Users need not have to explicitly grant storage access to MaaS360 before accessing files in the Secure Viewer and Editor on Android 11 or later versions.

Force app configuration feedback at device level >>

MaaS360 adds a new device-level action **Force App Config Feedback** to allow administrators to force the device to retrieve app configuration feedback from Google as quickly as possible and display it in the MaaS360 portal. Administrators can issue this action up to 3 times in 24 hours for a device.

Switch to a strict scheduler to schedule background tasks >>

AlarmManager and JobScheduler are among the popular methods supported in Android to schedule recurring background tasks. In the previous releases, MaaS360 used JobScheduler by default to report device heartbeat to the MaaS360 portal. In 10.81, MaaS360 adds a new policy setting: **Use Strict Scheduler for Heartbeat** to allow administrators to switch to AlarmManager, a stricter scheduler to execute background tasks such as device heartbeat. AlarmManager is strict in that the job is executed at the scheduled time even though the device is inactive, resulting in a battery drain. JobScheduler is optimized by the operating system to perform tasks when the device is charging, idle, or connected to a network.

Status of the System apps reported to the MaaS360 portal >>

If the System apps are distributed to the devices via App Catalog, the status of those apps is reported to the MaaS360 portal and displayed on the Device Summary > App Distributions page.

Platform

Addition of Custom Attributes section in the Device Summary >>

In addition to the existing device details in the Device Summary page, a new section called Custom Attributes is added that shows all device custom attributes that are defined by administrators. Administrators can now easily view and modify custom device attributes from the Device Summary page. The existing Custom Attributes page continues to show both MaaS360 defined and administrator defined custom attributes.

Search for devices with empty and non-empty attributes in Advanced Search >>

In this release, 2 new search criteria namely **Is Empty** and **Is Not Empty** are added in the Advanced Search condition. Previously, searching for devices that have empty and non-empty attribute values for any of the search categories was not possible. With these 2 search criteria, you can now search for any devices that have empty or null values and non-empty or non-null values for any of the attributes in the search condition. Example: You can search for users whose user groups value is empty, search for devices whose MaaS360 license status is not empty, and so on.

Support to filter users list in the User Directory based on users with devices and without devices >>

MaaS360 improvises the filtering capability in the User Directory page to help Administrators view users list based on users with devices, users with no devices, and all users in the customer account. Previously, "**Hide users with no devices**" option was available that would list only users with devices that are associated with the user account. Effective this release, Administrators can also view users with no devices that are associated with the user account. The "Hide users with no devices" is deprecated from this release and following 3 options are added:

- **All Users**: User Directory page shows all users in the customer account. This list includes both users with devices and without devices that are associated with their user accounts.
- **Users with Devices**: User Directory page lists only users that have devices that are associated with the user account.
- **Users without Device**s: User Directory page lists only users without devices that are associated with the user account.

Based on the option that is selected, User Directory page displays relevant users and Administrator can export the user details by using the **Export** option in the User Directory. This way, Administrator can view users with no devices as well in the User Directory page.

Improved ways to get new user login password >>

To ensure password security compliance, MaaS360 adds a new way on how user password is communicated to a local user during new user creation and password update scenarios. This change is applicable for manually set user password and auto-generating user password methods in the User Password Settings that are listed in **User Settings** page. Following changes are introduced in the User Password Settings.

- A new setting **Send password to user's email** that is added as a checkbox under **During User Account Creation (Manually set User password)**. If this checkbox is enabled, then, new users continue to receive the portal login password over welcome email. If unchecked, then, the welcome email sent to user does not include the login password and shows the following message: 'Please contact corporate administrator for the password'. New users can get the login password by contacting the corporate administrator. By default, this checkbox is enabled for existing customers so the new user creation process is unaffected and user can continue to receive password over email. For new customers, the checkbox is unchecked by default.
- **User account creation (Autogenerate User password)**: In this case, the password reset link is sent to the new users in the email that is sent following the welcome email. Using this link, users can set the MaaS360 account password. Even in case of password reset request, the password reset link is shared with user over email to set a new password. This workflow change is applicable to both new and existing customer accounts. Previously when this setting was chosen for user password setting, login password was shared over email and when user logs in to EUP, a prompt to change password was shown by using which user could set a new login password.

MaaS360 supports IBM's use of inclusive language in technology

IBM has launched an initiative to identify and replace terminology that promotes racial and cultural bias. MaaS360 aligns with IBM values in embracing the use of inclusive language by identifying and replacing racially and culturally biased terms in our product and documentation.

While IBM values the use of inclusive language, terms that are outside of IBM's direct influence, for the sake of maintaining user understanding, are sometimes required. As other industry leaders join IBM in embracing the use of inclusive language, IBM will continue to update the product and documentation to reflect those changes. To learn more about this initiative, see the Words Matter blog post on ibm.com.

Analytics

General availability of User Risk Management feature >>

MaaS360 announces general availability of User Risk Management feature to all new and existing customers. The feature offers a holistic view of the risk that is associated with each user by evaluating security and compliance through a device-centric approach whether a device is in or out of compliance. To gain access to user risk management dashboard, customers must enable this service from **Setup** > **Services** page and enable **User Risk Management**. The feature offers **Risk Rule Configurator** and **Security Dashboard** to define and evaluate risk incidents. To view Risk Rule Configurator and Security Dashboard in the MaaS360 portal, go to **Security** under the **Security Management** section.

The Risk Rule Configurator offers 14 predefines rulesets using which Administrator can customize the risk model to identify the risk incidents according to their organization's needs. The Security Dashboard gives an overview of the risky users, risky devices, total risk incidents, and the average risk score in the organization. Administrators can drill down to the risky users and devices and get a comprehensive overview of the incidents committed by a single user with the user summary page.

Enhanced UI dashboards and near-real time reporting for Mobile Data Usage Overview and Mobile Data Usage Analysis reports >>

MaaS360 offers improved UI experience for Mobile Expense Management reports and are available to all customers now. The functionality of the report remains the same as in previous user interface. The UI design elements are enhanced to offer best user experience with reporting. In addition to the enhanced UI, following capabilities are also offered;

- To easily access the subscription settings and UI settings configuration, an option '**Subscription settings**' is added in the data usage overview and data usage analysis reports page. On the click of this option, you are directed to the **Analytics** section under the Administrator Settings where you can configure the subscription settings for each of these reports.
- These reports are near real-time; any updates to the mobile data usage on devices are almost instantaneously reflected in the reports.
- The report dashboard shows a table icon, which when clicked shows both the chart data and the table data for the respective reports.

Near-real time reporting for Basic Apps Inventory and Advanced Apps Inventory reports >>

With the real-time reporting capability, Basic and Advanced Apps Inventory reports are now almost near real-time. Any updates in the statistical overview about app usage and app performance for managed and unmanaged apps on the devices are almost instantaneously reflected in these report dashboards.

Windows

New Microsoft Defender Device Guard policy >>

MaaS360 adds support for Microsoft Defender Device Guard (Device Guard) settings in the Windows MDM policy. The Device Guard settings allow administrators to configure settings that protect system integrity (System Guard) and credentials (Credential Guard) on Windows 10 devices.

The System Guard settings protect and maintain the integrity of the system as the system starts and validates that system integrity was maintained through local and remote attestation.

The Credential Guard settings use virtualization-based security to prevent unauthorized access that can lead to credential theft attacks by protecting NTLM password hashes, Kerberos Ticket Granting Tickets (TGT), and credentials stored by applications as domain credentials.

The Device Guard settings also protect devices on the next device reboot by using virtualization-based security features such as Secure Boot that check that a device boots authorized code and prevents bootkits and rootkits from installing and persisting across reboots, and hardware-based security features such as Direct Memory Access (DMA) that provide isolation and protection against malicious DMA attacks during the boot process and during the runtime of the operating system.

Windows 10 and Windows Server version 20H2 support for enforcement rules for Windows device compliance >>

MaaS360 now supports Windows 10 and Windows Server version 20H2 when you configure and assign compliance rules to Windows devices at the device level, group level, and during device enrollment.

What's New Since 10.80 Release Summary

Version 10.80.cd.16022021 Released 16 February 2021

Device range support option now available in Windows Bulk Provisioning Tool configuration wizard

MaaS360 now provides an option in the Windows Bulk Provisioning Tool configuration wizard that allows users to choose the number of Windows 10 devices that they want to enroll at the same time in the MaaS360 Portal.

With the new **Choose number of devices for enrollment** option, the estimated device enrollments occur over the following selected periods of time:

- - Immediately for less than 10 devices
  - 10 minutes for 11 - 100 devices
  - 30 minutes for 101 - 500 devices
  - 60 minutes for 501 - 1000 devices
  - 120 minutes for more than 1000 devices

Based on how you use the the Bulk Provisioning Tool (as an image or as an executable), see step 3 in the following topics for more information:

- https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/pag_source/tasks/bulk_provisioning_configure_imaging_process.htm
- https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/pag_source/tasks/bulk_provisioning_creating_executable.htm

Cloud Fixes Summaries

MaaS360 Cloud Fixes Summaries

November 2021 Daily Fixes Summary

MaaS360 Daily Fixes - November 2021

Fix #	Description	Date released
43706	Azure AD conditional access configuration did not reach the device due to incorrect MaaS360 app configuration.	02-November
43606	MaaS360 did not load the list of portal administrators in the Setup > Administrators workflow.	10-November
43770	After restarting the MaaS360 VPN app, Android devices could not connect to VPN.	10-November
43752	The devices in a group were not marked inactive even though the **Automated Device Hide** was turned on for that group	23-November

October 2021 Daily Fixes Summary

MaaS360 Daily Fixes - October 2021

Fix no	Description	Date released
43544	The administrator could not enable the **Identity and Access Management** > **IBM Security Verify** service.	04-October
43268	Android device users were unable to authenticate against their Microsoft Office 365 accounts on Secure Mail.	07-October
43363	Administrators could not publish a Windows MDM policy after uploading a certificate.	08-October
43627	Windows 10 Home enrollment redirects to a blank page instead of the Windows Home enrollment workflow.	08-October
43594	The administrator did not receive notifications after the new devices were enrolled.	08-October
43137	Automatic deletion of inactive users and devices failed.	12-October
43294	The administrator was unable to set the maximum duration to stay logged in during the session inactivity under Setup > Settings > Administrative settings > Advanced > Logout administrator sessions.	13-October
42606	Activated devices were not included in the App Inventory reports.	13-October
43580	Fixed a spelling mistake in iOS MDM policies.	21-October
43674	After Enabling License Management, the self enrollments using local authentication failed.	22-October
43767	App distributions failed on newly enrolled devices.	22-October
43698	After submitting a bulk policy change, policies were stuck at **Needs publish** status.	26-October

10.83 Release Fix Summary

The following customer issues were fixed in the 10.83 release:

Fix number	Description
39000	Fixed an issue where the advanced search/device group condition for the manual enrollment method did not return the expected devices in the search results.
42497	Fixed an issue where a new app version name was not updating on a device, but displayed the new app version name in the MaaS360 Portal for the device.
42172	Fixed an issue where the Administrator page was not loading in the customer's Portal.
43421	The policy change was not applied to the devices.
43326	The **Work Native** tag was displayed instead of **Device Owner** in the Android Enterprise Browser policies.
43171	Location authorization was set to **Always Allow** and the end-user could not change it.
43167	The Azure multi-factor authentication (MFA) was not supported for **Enroll on Behalf of**.
43092	Work Profile on Company Owned (WPCO) devices entered Factory Reset Protection mode even though FRP was not enabled in MDM policies.
42884	Background location access reminders were displayed on Android 11+ devices.
42871	After deploying WiFi configuration with the %password% variable, devices prompted for the corporate password. MaaS360 removed the misleading subtext under the Authentication Password field in the WiFi configuration policies.
41478	The MaaS360 Mail app could not be installed on the device after the enrollment.

September 2021 Daily Fixes Summary

MaaS360 Daily Fixes - September 2021

Fix no	Description	Date released
43401	MaaS360 populated usernames in the Email address field for the admin accounts that were auto-provisioned through Active Directory. As a result, the admin accounts did not receive the two-factor email that is used to log into the MaaS360 portal.	01-Sep
43449	The device groups took longer than usual to load.	02-Sep
43357	The MaaS360 VPN app could not connect to VPN due to certificate verification failure.	22-Sep
43554	Administrators could not add iOS 15 to the OS compliance rules.	22-Sep
43462	Administrators could not view the Azure AD Integration menu in the MaaS360 portal.	27-Sep
43438	The primary admin was unable to add/edit roles for new admins.	28-Sep
43408	Administrators could not change the policies applied to groups. When the admin deleted and recreated the group, the assigned policies for that group were restored.	30-Sep
43294	Administrators could not set the maximum duration to stay logged in during session inactivity under **Setup** > **Settings** > **Administrative settings** > **Advanced** > **Logout administrator sessions**.	30-Sep
43546	The web app was not removed on the device after the app was deleted in the App Catalog if the option Remove on Stop Distribution was not selected.	30-Sep

August 2021 Daily Fixes Summary

MaaS360 Daily Fixes - August 2021

Fix number	Description	Date released
42465	The usage policy displayed on the enrollment screens did not respect the formatting in the HTML file uploaded by the admin in the MaaS360 portal.	03-August
43227	When setting up Azure conditional access (beta), the partner compliance setup in Azure displayed the partner status **Connection lost** for the MaaS360 app.	04-August
43179	MaaS360 displayed a blank window when the administrator tried to stop the distribution through the App Summary page after distributing apps to 1000+ devices.	05-August
43139	The error message **App Deletion Failed** was displayed when the administrator tried to delete an app on macOS devices.	05-August
43246	When the administrator tried to change the Compliance Logs filter, the Compliance Logs Data page froze.	06-August
42859	The administrator could not clear the Cloud Extender user authentication alert.	20-August
42645	The administrator could not remove MDM control on devices.	20-August
42163	Hardware Inventory reports were incorrectly sent to the recipients that no longer subscribe for the email delivery.	25-August
43160	MaaS360 takes longer than usual to display LDAP user groups.	27-August
43379	MaaS360 portal displayed incorrect email address format for auto-provisioned AD administrator accounts.	27-August

July 2021 Daily Fixes Summary

MaaS360 Daily Fixes - July 2021

Fix number	Description	Date released
43095, 116620	If the settings **Allow users to remove** or **Remove on stopping distribution** were not enabled, users could not delete the web apps from the device even though the apps were removed from the App Catalog.	07-Jul-21
116108	The Android Enterprise policy setting **Allow cross-profile apps** did not apply to the device after publishing the policies.	12-Jul-21
42697	The devices enrolled through Apple DEP did not report usernames and email addresses assigned to them.	13-Jul-21
43145	Multiple iOS devices were flagged as non-compliant for no specific reason.	19-Jul-21
42074	The administrator added the same VPP token twice and could not disable the new token in the MaaS360 portal.	23-Jul-21
43105	Multiple new app recommendation emails were sent to the customers when the Send Email option was enabled during the app distribution.	28-Jul-21
43202	Google SafetyNet Attestation failed on multiple devices.	28-Jul-21
43091	Customers could not activate **Exchange and O365 integration** under Enterprise email integration in the Services tab.	28-Jul-21
38851	Data was not shown in the MaaS360 Services tab for the SPS Overview report.	30-Jul-21

June 2021 Daily Fixes Summary

MaaS360 Daily Fixes - June 2021

Fix number	Description	Date released
42839	The web apps remained on the devices even though they were deleted in the App Catalog.	15-Jun-2021
116374	The Persona policy that was applied to the device was not shown in the Device > Summary tab.	28-Jun-2021

May 2021 Daily Fixes Summary

MaaS360 Daily Fixes - May 2021

Fix number	Description	Date released
42789	The APIs Get Group for Device and Get Users and Device Groups returned inaccurate information.	11-May-21
42732	When the App Catalog Icon was updated via MaaS360 portal > Settings > iOS App Catalog, the icon was not pushed to the App Catalog on the devices.	12-May-21
42758	When the administrators enabled Trusteer and published the iOS policy, the action failed and the policies did not reach the devices.	12-May-21
42769	Administrators could not delete policies in the MaaS360 portal.	13-May-21
42558	An error message was displayed and administrators could not view their reports in the Reports > PC security workflow.	17-May-21
42609	The enrollment of devices in Device Owner mode with the MaaS360 token and QR code failed.	18-May-21
42739	After the OEMConfig configuration was pushed down to the Zebra device, the device went through a factory reset and disabled management via QR or ZT.	25-May-21
42549	The VPP apps were stuck at the pending updates state and failed to reach the devices.	27-May-21

10.82 Release Fix Summary

The following customer issues were fixed in the 10.82 release:

Fix number	Description
42222	Some of the Android devices received old app configurations.
42752	The mention of racial terms was found in the Android MDM Policy > Configure Restricted Applications workflow. **Note**: In an effort to promote inclusive language, MaaS360 drops the use of Whitelist/Blacklist and replaces these terms with Allowlist/Blocklist across all workflows in the MaaS360 Portal.
42564	Only a portion of the screen was displayed during the remote view session on Honeywell devices that were enrolled in Device Owner mode.
42538	When administrators tried to upload a URL to push a .bfa file through the Docs page in the MaaS360 Portal, an error message was displayed and the URL could not be uploaded.
42376	An incorrect version of the iOS B2B app was displayed in the MaaS360 App Catalog.
37555	The System Preferences panes: Apple ID and SideCar were grayed out by default after enrolling macOS Catalina devices.
36879	The end-user App Catalog was unavailable on iOS devices.
42954, 42581, 41972	When administrators tried to open the App Summary page, a progress indicator was shown and then after a period of time a Gateway Timeout error message was displayed.
42665	An error message was displayed when uploading large .apk files to the MaaS360 Portal.
41235	After app wrapping, the app stopped making web service calls from MEG.
41030	When Android Enterprise settings were changed, the change history displayed a change in the iOS App Management settings.
42675	The following pages in the MaaS360 Portal took longer than usual to render: • Devices / Inventory > Export • App Catalog / iOS Enterprise app - View
30202	When creating new administrators or editing an existing administrator account, the Roles page lists all available administrator roles. The roles with duplicate names led to errors when a partner chose roles for assigning to administrators. Hence, text to describe the hierarchy is added for roles with duplicate names. Using this hierarchy, correct roles can be assigned to administrators during add and edit administrator workflows. Following example, help texts are shown on hovering over the role names. • Administrator- No inheritance specified in this case since this role is inherited from the immediate partner's role. • Administrator (Inherited from 0)- Inherited from 0 (Fiberlink Master Account) • Administrator (Inherited from <example account number 1122334455>)- Inherited from 1122334455 (level1partner under 11122233) • Administrator (Inherited from <example account number 11122233>)- Inherited from 11122233 (level2partner under 66622211)
42749	Windows devices were not updated when changes were made to the Windows MDM Update Management policy.
42246	Windows 10 Home devices were not enrolling correctly.
41566	Search wasn't working after enrolling Zebra devices.
42674	Show Criteria in device groups was not working in Safari and Chrome.
42586	Accessing Settings in the MaaS360 Portal was not working.
42454	The MaaS360 console was not displaying all the tabs in IE11.
42252	Customer was unable to assign roles.
42153	The MaaS360 Portal API documentation was incorrect.
42001	Gateway timeout error.
41426	Searching in the MaaS360 Portal was not working.
41057	During userless enrollment, the terms of use that was set in the Persona policy did not appear after signing in.
40911	Limiting self-enrollment to specific user groups was not working (SAML authentication with Android Enterprise PO device).
42206	Alert center email messages issue.
41693	Unable to export the Administrator Login report from the MaaS360 console.
41336	Customer was not receiving SMS texts for 2 Factor Authentication (2FA).
42462	Customer couldn't remove SSM association from accounts.

April 2021 Daily Fixes Summary

MaaS360 Daily Fixes - April 2021

Fix number	Description	Date released
41652	The pending Windows OS patches were not displayed in the MaaS360 portal.	1-Apr-2021
114803	After updating the iOS Services Hostname in Settings > Advanced > Corporate Support, the setting automatically reverts to the Account Name.	1-Apr-2021
41680	The notification badge was not shown on the MaaS360 app in kiosk mode.	1-Apr-2021
42160, 42294	An error message was displayed when loading mobile metrics report for Apps.	05-Apr-2021
109668, 42601, 42611, 115042	Multiple policies were stuck at pending bulk edit status.	09-Apr-2021
42371	The **Revoke VPP License on Stopping Distribution** checkbox was automatically cleared on adding the app to the App Catalog.	09-Apr-2021
114862	The iOS apps were not removed when users signed out of the devices.	12-Apr-2021
42486, 42588	An invalid hostname error message was displayed while configuring IBM Security Verify.	12-Apr-2021
42483	When users tried to enroll iOS devices using SAML, the enrollments failed and an error message was displayed at the login.	15-Apr-2021
41213	The iOS group-level action **Ping All Devices** was missing.	22-Apr-2021
41693	Administrators could not export Administration Login Report in the MaaS360 portal.	22-Apr-2021
42566	An error message was displayed when the Windows apps were upgraded from the MaaS360 portal.	23-Apr-2021
42519	After the deployment, the identity Certificates failed to reach the device.	28-Apr-2021
42606	After deploying an Android enterprise app, MaaS360 displayed inaccurate installation status for activated (SPS-only) devices.	30-Apr-2021

March 2021 Daily Fixes Summary

MaaS360 Daily Fixes - March 2021

Fix number	Description	Date released
41988	An error message was displayed when administrators tried to update provisioning profiles for any app.	01-Mar-21
42122	The default Android MDM policy was unavailable in the MaaS360 portal.	02-Mar-21
42169	Some of the iOS public apps in the MaaS360 App Catalog did not receive the latest updates.	05-Mar-21
42437, 42499, 42347	Multiple policies were stuck at pending bulk edit status.	18-Mar-21
42206	Administrators did not receive My Alert Center email notifications.	22-Mar-21
41787	A WorkPlace persona policy was shown to have been assigned to a user group even though the WorkPlace persona policies were disabled by the administrator.	22-Mar-21
114813	Android devices did not receive the latest version of the Android MDM policy.	22-Mar-21
42252	The newly created custom roles were unavailable for the administrator that created those roles.	23-Mar-21
42241	Inaccurate installation status was displayed in the MaaS360 portal when the web apps were installed manually.	24-Mar-21
42489	The new iOS & iPadOS enrollments did not receive iOS App Store apps.	24-Mar-21
41514	MaaS360 will no longer sync the available iOS updates from Apple for non-supervised devices. For the supervised devices, MaaS360 will continue to display the available iOS updates in device summary > Hardware & OS > Available Updates.	
114784	After changing the topic of APNs, the APNs cert serial number was displayed as undefined and enrollment was going to pending state	

10.81 Release Fix Summary

The following customer issues were fixed in the 10.81 Release:

Fix number	Description
30783	Cloud-based integrations: Fixed an issue where SSO Conditional Access in the iOS MDM setting was not displaying data.
40495	Cloud Extender: Fixed an issue with the inability to perform actions on an ActiveSync record.
41413	Cloud Extender: Fixed an issue with Android devices showing unexpected Certificate Renewal Process actions.
41718	When the user license type VPP apps were distributed to the User Enrolled devices, the apps were not installed and the status was shown as Not Relevant.
41867	The newly enrolled Android Enterprise devices did not receive distributed apps.
39252	The Exchange Payload was not applied to macOS devices that were enrolled via DEP.
41514, 41255	MaaS360 no longer syncs the available iOS updates from Apple for non-supervised devices. For the supervised devices, MaaS360 will continue to display the available iOS updates in device summary > Hardware & OS > Available Updates.
41714	The code to bypass the activation lock was not generated and the clear activation lock action could not be issued when the MaaS360 portal language was set to French.
41936	An enterprise app wrapped with Android SDK crashed on all Android 11 devices that were enrolled in DA mode.
42050	The app custom attribute of URL type failed if the domain name was greater than 5 characters.
42069	The execution of the **Install App** API command failed.
42131	The bulk upload action to send enrollment requests to multiple users at once failed.
42135	In self enrollments, the device ownership that was selected in the End User Portal did not reflect in the MaaS360 portal.
40204	When adding apps from the Managed Google Play store, the app category name changed to uppercase and the spaces were replaced with underscores.
40649	Multiple scroll bars were displayed in the embedded Google iframes in the MaaS360 portal.
40821	When the same script with the same name was uploaded for multiple apps, the script was deleted on deleting one of the apps.
41487	The installation of a Windows app failed if the custom installation command exceeded 255 characters.
41557	The sensitive information in the QR codes that were used for Android Enterprise enrollments was not encrypted.
41635	The scheduled heartbeat communications stopped and devices failed to report to the MaaS360 portal. For more information on switching to a stricter scheduler, see https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/pag_source/concepts/mdm_policy_gde_ae_device_management.htm
41751	Some of the Zebra OEMconfig settings were not deployed to the devices.
41804	The app permissions email notification did not contain customer details, making it harder for the admins to figure out which account was referred to in the message.
41906	The deleted web apps were auto-installed on the devices.
41988	An error message was displayed when administrators tried to update provisioning profiles for any app.
42027	When the DEP devices were set to auto rename with the user attribute %Department%, the changes were not applied after the enrollment.
42064	The cloned macOS MDM policy could not be published.
42090	An error message was displayed when uploading a Windows Universal App Package (.appx) file.
42162	When the device was re-added to the device group, the apps that are assigned to that group were not installed automatically.
42032	Doc distribution expiry date and time were auto-updated even though those details were not specified during the distribution.
40911	Fixed an error where limiting self-enrollment to only specified user groups in the SAML authentication during device enrollment was not working. At the time of enrollment, error message that user does not belong to the user group was displayed on the device although user was member of the specified user group.
41693	Fixed an issue with exporting administrator login report as a CSV file or excel file. On the click of CSV or export, the report was failing to download by spinning constantly for almost an hour with no report download.
42135	The issue with device ownership details not displaying when the user enrolled the device from End User Portal (EUP) is fixed now. Whenever the user enrolled the device from EUP and defined the device ownership, this filed was still showing as 'Not Defined' in the portal under Device Hardware Inventory details.
38500	If one or more users exists with same email address and if enrollment requests are created for all these users and in case wrong enrollment request is considered by a user, then, authentication must fail and no new enrollment enrollment should be created but this expected behavior turned out false and new enrollment enrollment got created in case of Passcode authentication type, which is fixed now.
41866	In the Administrators page, filtering data by administrator status as 'inactive' or list 'all' administrators was showing parsing error if count of such administrator details exceeded 1000 number that is fixed now.

Fix number	Description
41984	Corporate credential administrators with administrator status as inactive were unable to log in to MaaS360 portal and error that credentials were incorrect or account is not provisioned was displayed. The issue was due to mismatch between the active directory setup and group name that is configured in the portal. The issue is fixed and administrator can log in to the portal. The issue is when special character is used in the group name that leads to mismatch of group name in active directory and in the portal.
41622	The email template that is sent out during device enrollment request had the body of the email that was duplicated and showing twice, which is fixed.
41829	In the Advanced Administrator Settings > Login Settings, to automatically create new administrator accounts and to update roles based on user groups, there are two separate fields that are provided for user groups and to select roles.
41839	On hovering over the Summary tab Device view, the summary details were displayed which remained unclosed on the screen even when other menu options in the screen were selected and this issue is fixed now.
41868	The device enrollment request email included one time passcode for a SAML enrollment method that should not be the case and the issue is fixed.
42087	In the Apps Inventory reports page, for the selected language as Japanese, the Subscription Settings option showed in English instead of Japanese and this issue is fixed now.

February 2021 Daily Fixes Summary

MaaS360 Daily Fixes - February 2021

Fix number	Description	Date released
40867	The status of the ActiveSync Mailbox Approval State was stuck at Blocked after the device returned to the compliance state.	03-Feb
41057	During the userless enrollment, the usage policy was not shown after the sign-in.	04-Feb
41942	The inactive user and device records were not deleted even though the MaaS360 portal was set up to delete users and device records after 90 days.	05-Feb
40613	The device Action and Events page took a long time to load.	08-Feb
41896	The Hardware Inventory did not return results and displayed **Not enough data to display chart** message.	10-Feb
41456	MaaS360 displayed inaccurate entries in the app update history.	11-Feb
42192, 42276	Multiple policies were stuck at pending bulk edit status.	11-Feb
41818	Customers could not take remote control of Samsung devices using the MaaS360 Remote Support app.	12-Feb
41988	An error message was displayed when updating the provisioning profile of an app.	15-Feb
42091	When the administrator tried to convert an account to a script only user, the action failed and an error message was displayed.	15-Feb
39696	An iTunes App Store app was stuck in the App Processing state after the distribution.	16-Feb
41790	Some .msi and .exe packages failed to install on Windows devices.	19-Feb
40406	The execution of scripts failed on Windows devices.	19-Feb

January 2021 Daily Fixes Summary

MaaS360 Daily Fixes - January 2021

Fix Number	Description	Date released
41798	When the administrators tried to save the auto-logout admin session settings, an error message was displayed and the changes were not applied.	06-Jan
41925, 42033	After publishing the bulk edit changes, the policies were stuck at the Pending Bulk Edit status.	06-Jan
41983	An error message was displayed and Android enterprise apps were not installed on newly enrolled devices.	06-Jan
41625	A portal administrator could not access Setup > Administrator workflow.	07-Jan
41546	When a compliance rule was created to monitor OS version changes, the administrator received email notifications every 30 minutes even though there was no change in the OS version.	08-Jan
114105, 114106	After upgrading to the latest version of the User Visibility module, some of the users were marked as inactive.	08-Jan
41737	The Unified Enrollment settings were changed inadvertently on updating the auto-update app settings.	15-Jan
41610	The Trusteer Malware service was missing under the Installed Services in the app detail view.	15-Jan
133406	Secure Chat was unavailable on iOS and Android devices.	21-Jan
41941	A user group was only partially deleted and not displayed on the UI.	20-Jan
41840	Users could not set the language of the End User Portal logon page to Japanese.	22-Jan
42071	An app could not be signed with a new certificate.	25-Jan
41742	The installation of an app failed when distributed via groups.	29-Jan

December 2020 Daily Fixes Summary

MaaS360 Daily Fixes - December 2020

Fix Number	Description	Date Released
106077	Users could change the pre-defined username on the Unified enrollment screens.	06-Dec-2020
41733	Usernames were merged as one record when imported from multiple domains from Azure AD.	08-Dec-2020
41805	After publishing the bulk edit changes, the policies were stuck in the Pending Bulk Edit status.	11-Dec-2020
41773	Email notifications were automatically sent to users whenever EULA was updated.	11-Dec-2020
41565	The URL in the wrapped app was truncated when opened in Secure Browser.	14-Dec-2020
41636	Some apps in the App Catalog failed to load in the App Catalog.	15-Dec-2020
113766	The configuration of GSuite account failed.	15-Dec-2020
41816	The identity certificate expiration message was displayed in MaaS360 device settings.	16-Dec-2020
41542	The device-based enrollment of Bluebird devices in Android Enterprise mode failed.	17-Dec-2020
41150	iOS devices reported inaccurate model numbers to the MaaS360 portal.	17-Dec-2020
38597	The latest OS Patch Updates were not deployed to Windows 10 devices.	17-Dec-2020
41888	Cloud Extender User Visibility Module did not upload incremental data to the portal.	17-Dec-2020
41704	The distribution of multiple apps at once from the App Catalog failed.	18-Dec-2020
41867, 114016	When the approved apps were distributed to the newly enrolled Android Enterprise devices, the apps appear in the end-user App Catalog, but users could not install them from the Play Store.	18-Dec-2020
41760	The SPS/activated devices reported inaccurate installation count to the MaaS360 portal.	22-Dec-2020

iOS Release Summaries

MaaS360 iOS App & SDK Release Summaries

iOS Secure Browser 3.60.30 Release Summary

MaaS360 makes the MaaS360 Secure Browser app version 3.60.30 available on iTunes on 20 December 2021.

This release includes the following fixes:

Fix #	Description
44074	The VPN setting on the device was automatically turned off and the Secure Browser app failed to connect to MaaS360 Enterprise Gateway (MEG).
43156	When the App Lock mode is enabled, the devices were stuck at the configuration screen on the Secure Browser app during the enrollment.

Note:

- Requires MaaS360 for iOS app version 4.81.3 and MaaS360 Secure Browser app version 3.60.30 for this fix to work.
- After the upgrade, users are prompted to install the VPN profile.

iOS 4.81.3 Release Summary

MaaS360 makes the iOS app version 4.81.3 available on iTunes on 20 December 2021.

This release includes the following fixes:

Note: Requires MaaS360 for iOS app version 4.81.3 and MaaS360 Secure Browser app version 3.60.30 for this fix to work.

Fix #	Description
44074	The VPN setting on the device was automatically turned off and the Secure Browser app failed to connect to MaaS360 Enterprise Gateway (MEG).
43156	When the App Lock mode is enabled, the devices were stuck at the configuration screen on the Secure Browser app during the enrollment.

Note:

- Requires MaaS360 for iOS app version 4.81.3 and MaaS360 Secure Browser app version 3.60.30 for this fix to work.
- After the upgrade, users are prompted to install the VPN profile.

iOS 4.80 Release Summary

MaaS360 makes the iOS 4.80 app beta available on TestFlight on 30 November, 2021.

Additional control for showing blocked images from external domain emails >>

By default, when the remote images from external domains are blocked by the administrator, the remote images in emails are automatically hidden. Effective 10.84, MaaS360 adds additional controls to allow users to view the images by tapping the banner at the top of the email when the remote images are blocked.

Consistent user interface for authentication screens >>

MaaS360 now displays a unified authentication screen across all platforms. In 10.84, MaaS360 extends the consistent authentication UI from Shared device login workflow to Forgot PIN, password-protected documents, and app sign-in workflows.

Note:

- Requires MaaS360 for iOS app version 4.80+.
- This feature is not enabled by default. Contact the MaaS360 Support team to get this feature enabled for your account.
- When the authentication mode is set to Corporate (Azure), users are redirected to the Azure portal for authentication during enrollment. For Azure enrollments, administrators should have the unified authentication feature enabled and the authentication via Azure AD allowed for MaaS360 to display the unified authentication screen.

Defect fixes

Defect	Summary
43121	After migrating from basic to Modern Authentication, Secure Mail did not prompt for Modern authentication even though SSO was enabled in security policies.

iOS 4.70 & Secure Browser 3.60 Release Summary

The MaaS360 for iOS app version 4.70 was available on iTunes on 11th November 2021.

The MaaS360 Secure Browser version 3.60 was available on iTunes on 14th November 2021.

Defects Fixed

iOS 4.70 App Defect

Defect	Summary
42996	When the administrator published a policy multiple times in a day, MaaS360 did not display the latest policy information pertaining to some devices in the MaaS360 portal.

iOS 4.70 and Secure Browser 3.60 Defect

Defects	Summary
43054	iOS MEG support of Apple WKWebView VPN profile is conflicting with existing CheckPoint VPN profile

iOS Secure Browser 3.50 Release Summary

MaaS360 makes the Secure Browser app version 3.50 available on iTunes on 08 September 2020.

iOS 15 Zero-day support >>

MaaS360 continues to support all the iOS Secure Browser app features on iOS 15 devices.

Defect Fixes

Defect	Summary
42229	A corporate website was not rendered on the Secure Browser app when launched via a VPN connection.
42608	The **Open in New Tab** pop-up window was displayed on long pressing the dropdown menu items in the Secure Browser app.

iOS 4.60 Release Summary

MaaS360 makes the iOS app version 4.60 available on iTunes on 07-September-2021.

- **iOS 15 zero-day support >>**

With iOS 15 zero-day support, new iOS 15 devices will enroll with MaaS360, and the existing devices upgrading to iOS 15 will continue to work.

Impact on MaaS360 notifications when Notification Summary is enabled >>

With iOS 15, Apple introduced Notifications Summary, wherein iOS smartly compiles all the less-urgent notifications and delivers to users in batches at the time they choose. **Note**: If users add the MaaS360 for iOS app to the Notification Summary, iOS delivers MaaS360 notifications at the time the notification summary is scheduled to appear. As a result, the expected behavior is that users will miss out on important alerts such as email and calendar notifications.

- **Minor bug fixes and improvements**

iOS Secure Editor 2.90.8 Release Summary

MaaS360 makes the iOS Secure Editor app version 2.90.8 available on iTunes on 6-August-2021.

- MaaS360 adds group-based support for Azure AD Conditional Access.

Defect Fixes

Defect #	Description
43245	After exporting files from the MaaS360 app, the Secure Editor app failed to save files to the personal drive the first time they are saved. Users had to manually save the file to the source and then perform the save action again to be able to save the file. Effective Secure Editor app version 2.90.8, the files are saved to the personal drive when the save action is performed.

iOS 4.50.18 Release Summary

MaaS360 makes the iOS app version 4.50.18 available on iTunes on 30-July-2021.

- MaaS360 adds group-based support for Azure AD Conditional Access.

iOS 4.40 Release Summary

MaaS360 makes the iOS app version 4.40 beta available on TestFlight on 08-June-2021.

Retrieve device serial number through barcode >>

MaaS360 adds a barcode to the MaaS360 Support container, allowing users to retrieve the device serial number by scanning that barcode.

Fixes

- Fixed some of the issues that caused the MaaS360 app to crash in the background. With this release, TestFlight users will notice fewer background crash prompts as compared to previous versions.

Defect number	Summary
42941	MaaS360 displayed duplicate email signatures on Reply All, Forward, and Reply screens.
42880	In the compose mail screen, users could not drag and drop mail recipients between To, CC, and BCC fields.

iOS Secure Brower 3.45 Release Summary

MaaS360 makes Secure Browser app version 3.45 beta available on iTunes on 02-June-2021.

Multitasking support for iOS Secure Browser app >>

MaaS360 extends split-view multitasking support for iOS Secure Browser. This feature allows users to use iOS Secure Browser app alongside other multitasking enabled iOS apps or with a non-multitasking iOS app in the Slide Over mode. For example, you can view the Secure Browser app and Apple Notes (or any other Native app) side-by-side at the same time.

Note:

- In multitasking mode, dismiss any alerts presented by websites in the Secure Browser app before changing the screen size. If you change the screen size without dismissing the alert, the app will crash.
- MaaS360 announces end of support for iOS 11 or earlier devices. Effective iOS Secure Browser app version 3.45, the new updates to the Secure Browser app can only be installed on iOS 12 or later devices.

Defect Fixes

Defect	Summary
42399	When the users created a webclip, Secure Browser automatically redirected to https instead of http
42400	When the browsing history was deleted, the websites in the Frequently Visited Pages and Recently Closed Page were not cleared.

Known issues

- When scanning the QR code in the multitasking mode, the camera will not be displayed.
- Some of the SDK screens such as email logs do not support multi-tasking.

Limitations

- After exiting the multi-tasking mode, the Secure Browser app is launched in the full-screen mode by default.
- In the multitasking mode, the keyboard toolbar does not adjust according to the keyboard.

iOS 4.30 Release Summary

MaaS360 makes the iOS app version 4.30 available on iTunes on 20 May 2021.

Custom font size support for Mail detail view >>

MaaS360 auto-adjusts the Mail detail view according to the system font size on iOS devices.

Defect Fixes

Defect	Summary
42428	Users were unable to open the Google Meet app via the meeting link sent on the MaaS360 calendar on iOS devices. With this fix, the meeting URL successfully redirects to the Google Meet app when the application is installed on the device and then the advanced property **calOtherMeetingURLHosts** is pushed via Persona policies.
42218, 41944, 42363	Secure Mail detail view did not respect the System font size settings on iOS devices.
42716	When users forwarded an email with an attachment via Secure Mail before downloading the attachment in the original mail, the recipient could not view the file content.

iOS Secure Editor 2.80.21

MaaS360 makes the iOS Secure Editor app version 2.80.21 available on iTunes on 15 April 2021.

Conditional access to Microsoft approved client apps >>

MaaS360 extends conditional access support to Secure Editor. With this support, administrators can restrict access to Microsoft-approved cloud apps only from trusted and compliant devices. To leverage Conditional Access, MaaS360 uses the Microsoft Authenticator broker app to register devices in Azure Active Directory. After the registration, the device compliance status is forwarded from MaaS360 to Azure AD where conditional access makes decisions to grant or deny access to the Microsoft cloud apps.

Note:

- This feature is not available by default. Contact the MaaS360 customer support team to enable this feature for your account.
- It is recommended to enable this feature only on MaaS360 test accounts to avoid unexpected Azure Device Registration prompts on all the devices enrolled in the organization.

iOS 4.20 Release Summary

MaaS360 makes the iOS app version 4.20 available on iTunes on 08 March 2021.

Note:

- Effective MaaS360 for iOS app 4.20, the enrollment/activation is terminated when an untrusted connection or proxy is detected on the device even if Certificate pinning is turned off.
- If Certificate pinning is enabled and the proxy is added, customers must disable SSL proxying for the MaaS central server before enrolling/activating new devices.

Note: The configuration of Microsoft services (OneDrive & SharePoint) failed on older agents due to an update from Microsoft. It is recommended to upgrade to the latest version of the MaaS360 for iOS app to avoid configuration failures.

Advanced external domain email restrictions >>

MaaS360 adds a new policy **Warn about attachments in emails from external domains** to allow administrators to configure a security alert for attachments in external emails. When enabled, MaaS360 displays a security alert on opening attachments to protect users from unintentionally opening attachments in emails that originate from external domains.

Conditional access to Microsoft approved client apps >>

MaaS360 adds support for conditional access to Microsoft-approved cloud apps based on the compliance status of the devices. To leverage Conditional Access, MaaS360 uses the Microsoft Authenticator broker app to register devices in Azure Active Directory. After the registration, the device compliance status is forwarded from MaaS360 to Azure AD where conditional access makes decisions to grant or deny access to the Microsoft cloud apps.

Note:

- This feature is not available by default. Contact the MaaS360 customer support team to enable this feature for your account.
- AzureAD Conditional Access feature is in preview mode from Microsoft. It is recommended to enable this feature only on MaaS360 test accounts to avoid unexpected Azure Device Registration prompts on all the devices enrolled in the organization.

Added new sign-in banner across Office 365 services >>

If the sign-in session is terminated, end-users can now use the Sign-in banner in the Office 365 Services (Office 365 Mail, SharePoint, and OneDrive) to re-authenticate the session. **Note**: The functionality is limited to Office 365 services that use Modern Authentication. Among the MaaS360 container apps, the Sign-in banner is shown only in the MaaS360 Email container.

During the shared device logout, users are not required to sign out of individual accounts manually from the logged-in Office 365 accounts.

Defect fixes

iOS SDK 4.00.000 Release Summary

MaaS360 makes the iOS SDK version 4.00.000 available on 10 February 2021.

1. **To comply with Apple guidelines, MaaS360 SDK will stop supporting DLP for the UIWebview host application and removes all references to the UIWebView. If your app still uses UIWebView in your project and you need DLP support for that app, then use MaaS360 SDK version 3.30.950 or lower.**
2. Added MEG 3.0 support. MEG 3.0 is not supported in Android and MaaS360 iOS SDK Cordova. For more information, see https://www.ibm.com/support/pages/node/6129267
3. The following features are not supported with MEG 3.0:

- Application-level SSL handling
- Resource-based cert pinning
- Cache credential
- Proxy with PAC without allowing the PAC domain in gateway settings is not supported. You need to allow the PAC domain / IP in the gateway setting in the persona policy.
- Xcode 12 is not supported in this release.

PIV-D 1.35.6 Release Summary

MaaS360 makes the PIV-D app version 1.35.6 available on iTunes on February 09, 2021.

- With PIV-D app version 1.35.6, MaaS360 stops clipboard use for passcode management to avoid the banner alerts on iOS 14 devices except for the scenarios wherein the end-user explicitly performs a paste operation.
- The passcode provided for the MaaS360 app is automatically applied to the PIV-D app and vice versa when both the apps are launched simultaneously.

iOS 4.10 Release Summary

MaaS360 makes the iOS app version 4.10 available on iTunes on 16 February 2021.

Defect Fixes

Defect	Summary
41998	MaaS360 app crashed when users tried to open an app with a deep link.
41354	Customers could not import documents from native Mail and Calendar apps to the MaaS360 Secure Container through **Import to MaaS360** share action menu.
41889	After changing the password in the Account settings, the account validation against the Traveler server failed and the Secure Mail app could not sync emails.

iOS Secure Browser 3.40 Release Summary

MaaS360 makes the iOS Secure Browser app version 3.40 available on iTunes on 17 February 2020.

Defect Fixes

Defect	Summary
41934	PDF files on an intranet site display distorted characters on MEG 3.0.
41449	The URL in the address bar could not be modified in the Secure Browser.
40978	The URLs in the Microsoft Outlook app that contain a port number could not be opened with Secure Browser.

Android Release Summaries

MaaS360 Android App & SDK Release Summaries

Android 7.71 Release Summary

MaaS360 makes the Android app version 7.71 available on the Play Store on 20 December 2021.

This release includes the following defect fixes:

Fix #	Summary
44085	Android devices could not launch in Kiosk mode.

Android 7.70 Release Summary

MaaS360 makes Android app version 7.70 beta on the Play Store on 09 December 2021.

Password complexity enhancements >>

MaaS360 extends the password complexity policy setting from Profile Owner to Device Owner devices. The **password complexity feature** sets device-wide password requirements in the form of predefined complexity buckets (High, Medium, Low, and None). If the administrator defines the password complexity policy setting, then the older passcode policies (Minimum Passcode Quality, Minimum Passcode Length) are not respected. **Note**: Supported on Android 12+ Profile Owner and Device Owner devices. Requires Android App 7.50+ for PO. Requires Android App 7.70+ for DO.

Advanced app compliance policies to control user-installed apps on managed devices >>

MaaS360 extends the **Configure allowed apps** and **Configure restricted apps by permission** settings from Device Admin to Android Enterprise policies. Administrators can use these policies to remotely control (allow/block) user-installed apps on managed devices.

- **Configure allowed apps**: When administrators configure allowed apps, all other user-installed apps on the device are disabled.
- **Configure restricted apps by permission**: Administrators can specify permissions that are not allowed on the managed devices. The user-installed apps that use restricted permissions are disabled until those permissions are revoked by the users from the device settings.

Note: These settings are not applicable to system apps, first-party apps, and apps installed via the App catalog.

Multicloud support for Modern authentication (MSAL) >>

MaaS360 upgrades the MSAL library for Android to provide the MaaS360 agent app the ability to support advanced multi-cloud scenarios. In the previous releases, the MSAL configuration did not support advanced Office365 resource endpoints such as https://outlook.office365.us. As a result, authentication to the Secure Mail app failed on Android devices. **Note**: Requires the MaaS360 for Android app version 7.70+.

Restrict personal accounts in Google Play >>

MaaS360 adds an advanced Android Enterprise policy setting **Restrict Personal Accounts in Google Play**. When this setting is enabled, users can add personal Google accounts to use services like Maps, Mail, or Drive, but they cannot use personal Google accounts to install Google Play apps. **Note**: Applicable for both GSuite & non-GSuite accounts.

Consistent Device Identifier for Android Enterprise enrollments >>

Google generates an enrollment-specific identifier for the device as a part of Android Enterprise enrollment. In the previous releases, a new identifier was generated whenever a device was enrolled, which left a trail of duplicate records when the same device was re-enrolled. Effective 10.84, a consistent device identifier is generated which remains the same for the device even if the work profile is removed and re-enrolled or the device is wiped and re-enrolled. Requires Android app 7.70+

Note:

- On Android 12+ devices, the consistent device ID is automatically generated for Android devices that are enrolled in Android Enterprise mode.
- On Android 11 and lower devices, administrators must set the custom enrollment attribute ***use_persistent_device_id*** to ***true*** to enable consistent device ID for Device Owner (DO) and Work Profile on Corporate Owned (WPCO) devices. For more information about enrollment attributes, see https://www.ibm.com/docs/en/maas360?topic=portal-additional-android-enterprise-enrollment-attributes

Work Profile enrollment flow changes >>

To generate a consistent device ID, MaaS360 introduces minor changes in the Work Profile enrollment flow. Effective 10.84, the authentication screen is displayed after the work profile creation.

- **Old flow** - EnrollmentInstrumentation > Authentication > WorkProfile Creation > Google Account Creation
- **New Flow** - EnrollmentInstrumentation > WorkProfile Creation > Authentication > Google Account Creation

Additional control for showing blocked images from external domain emails >>

When the remote images from external domains are blocked by the administrator, the remote images in emails are automatically hidden. Effective 10.84, MaaS360 adds additional controls to allow users to view the images by tapping the banner at the top of the email when the remote images are blocked.

Certificate pinning enhancements >>

In the third phase of series of enhancements, MaaS360 adds support to enforce Certificate pinning on all devices or specific user or device groups. When Certificate pinning is enabled for specific groups and devices, the server's certificate is pinned to MaaS360 apps only after persona policies reach the device. Administrators can configure the certificate pinning for Email, Gateway, and workplace apps through Persona policies irrespective of whether certificate pinning is turned on or off.

Android 7.61 Release Summary

MaaS360 makes the Android app version 7.61 available on the Play Store on 7th October 2021.

Defect Fixes

Defect	Summary
43629	Users could not access corporate websites on Secure Browser on Android devices running OS versions 7 or lower.
43770	After restarting the MaaS360 VPN app, Android devices could not connect to VPN.

Android 7.60 Release Summary

MaaS360 makes the Android app version 7.60 beta available on the Play Store on 20 September 2021.

User interface enhancements to more authentication workflows >>

- New user interface: MaaS360 adds new authentication UI for Shared device login, Forgot PIN, password-protected documents, and app sign-in workflows.
- Consistent user interface: MaaS360 extends the consistent authentication UI from Shared device login workflow to Forgot PIN, password-protected documents, and app sign-in workflows. **Note**: Requires MaaS360 for Android app version 7.60+. This feature is not enabled by default. Contact the MaaS360 Support team to get this feature enabled for your account.

Fixed parsing issue in .MSG files >>

MaaS360 uses the POI library for parsing the msg and RPMSG files. In this release, MaaS360 upgrades the POI library to fix parsing issues in .MSG files.

Fixed background location access notifications issue >>

During the Android Enterprise (DO and PO) enrollment, the MaaS360 for Android app granted itself Location permission in the background without allowing users to modify the permission from the device Settings. Effective OS version 11, Android started displaying periodic notifications to remind the users that the MaaS360 app has access to their location. To avoid the background location access reminders, MaaS360 now allows administrators to configure runtime permissions in a way that the Location permissions are controlled by the end-users. MaaS360 adds a new policy setting to mark devices as non-compliant if the MaaS360 app does not have location permission.

Enhancements to Android Enterprise runtime permissions >>

MaaS360 now allows administrators to control how Location, Storage, and Phone permissions are granted to the apps. In the previous releases, those permissions were auto-granted during the enrollment. MaaS360 removes the unsupported permissions, adds support to grant all permissions at once, and more.

Deprecation of Samsung Knox License (SKL) policy >>

Samsung makes premium Knox Platform for Enterprise (KPE) licenses available to all customers at no cost. See the announcement here: https://www.samsungknox.com/en/blog/knox-platform-for-enterprise-free-for-customers. In previous releases, customers had to purchase the premium Knox Platform for Enterprise (KPE) licenses and activate those licenses through security policies in the MaaS360 portal. Effective 10.83, MaaS360 removes the policy setting **Samsung Knox License (SKL)** from the MDM policies. **Path**: Android MDM policies > **OEM Settings** > **Samsung License Management** > **Samsung Knox License (SKL)**

Note: This change will be implemented as a part of DD after the 10.83 release. Customers who have already activated KPE Premium licenses through the MaaS360 Security policies must upgrade to the MaaS360 for Android app version 7.55 or later to avoid unexpected issues that might lead to re-enrollment of devices or license expiration error messages.

Trusteer Threat Management enhancements >>

MaaS360 includes new trigger events for the quicker detection of risk items on devices such as Root status change, Insecure Wifi detection, Malware detection, and so on. Effective 10.83, MaaS360 uploads the scan results to the MaaS360 portal in near real-time. In the previous releases, it took about 20 minutes for MaaS360 to upload the latest scan data to the MaaS360 portal. In addition to that, MaaS360 adds support for automatic uninstallation of the apps on Device Owner devices if the malware is detected.

Android 12 Zero-day support >>

When MaaS360 runs on Android 12, there will be behavior changes that impact some of the features in the MaaS360 app. MaaS360 first-party apps and SDK apps will continue to work on Android 12.

New custom command to remotely clear app data >>

In the previous releases, MaaS360 added custom command support, allowing administrators to execute remote actions on the managed Android devices. In this release, MaaS360 adds a new command to allow administrators to remotely clear the app data. **Syntax**: clear-app-data <comma-separated app IDs>. **Example**: *clear-app-data com.ibm.security.verifyapp, com.ibm.gts.banorte.epass*. **Note**: Requires MaaS360 for Android app version 7.60 or later. Supported only on Android Enterprise devices running OS version 9 or later. The action fails if the target apps are not installed on the device.

Removed ActiveSync support for Motorola email client >>

MaaS360 removes Motorola email client support from the Device Admin ActiveSync policies. As a result, administrators can no longer use Device Admin policies to configure ActiveSync on the Motorola email client.

Strict scheduler for device payloads >>

MaaS360 extends strict scheduler support from device heartbeat to payloads. With this support, MaaS360 uploads payloads in real-time. When this policy is turned on, the payloads upload timer strictly follows the value defined in the Data Collection Frequency policy setting.

Refactored code to stop requesting permissions during the Bulk Enrollment >>

In the previous releases, MaaS360 allowed customers to enable the MaaS360 app to request permissions during the enrollment process. Effective 10.83, the MaaS360 app requests all the required permissions at the runtime for Device Admin Bulk Enrollments.

AAPT2 enabled by default for Android app wrapping >>

In the previous releases, administrators had to use app wrapping parameters to enable AAPT2. Effective 10.83, AAPT2 is enabled by default for Android app wrapping. **Note**: Customers can continue to use the app wrapping parameters to set enableAAPT2 to false.

Track Wallpaper, Lockscreen, and APNS configuration status in Corporate settings >>

When administrators deploy Wallpaper, Lockscreen, or APNS restrictions to the devices, end-users can now easily track the configuration status in the Corporate settings in the MaaS360 app. **Note**: Requires MaaS360 for Android app version 7.60 or later.

Auto-installation of CA certificates on Android devices >>

MaaS360 now automatically installs the CA certificates on devices without requiring the users to manually install those certificates from the Corporate Settings in the MaaS360 app. **Note**: Supported on Android Enterprise devices and Samsung Device Admin devices. Requires MaaS360 for Android app version 7.60.

Android 7.55 Release Summary

MaaS360 makes the Android app version 7.55 beta available on the Play Store on 26 August 2021.

Android 12 Zero-day support >>

When MaaS360 runs on Android 12, there will be behavior changes that impact some of the features in the MaaS360 app.

App Catalog service exempted from billing when used for the distribution of first party apps >>

In the previous releases, when an app was distributed to the App Catalog, the App Catalog service was enabled, and customers were billed for using the App Catalog service. Effective 7.55, when the customers purchase first-party apps, they can distribute those apps to the App Catalog without being charged for using the App Catalog service.

List of supported first-party apps:

- MAAS360 APP = "com.fiberlink.maas360.android.control"
- OEM HELPER APP = "..." (Depends on OEM)
- MAAS360 DOCS = "com.fiberlink.maas360.android.docs"
- MAAS360 PIM = "com.fiberlink.maas360.android.pim"
- SECURE EDITOR = "com.fiberlink.maas360.android.secureeditor";
- SECURE VIEWER = "com.fiberlink.maas360.android.secureviewer";
- SECURE BROWSER = "com.fiberlink.maas360.android.securebrowser";
- KIOSK APP = "com.fiberlink.maas360.android.launcher";
- LENOVO KIOSK = "com.fiberlink.maas360.android.kiosk.lenovo";
- REMOTE_CONTROL = "com.fiberlink.maas360.android.remoteControl";
- MAAS360 VPN = "com.fiberlink.maas360.android.maas360vpn"

Note: Customers will be billed for using the App Catalog Service for apps other than first-party apps.

Support to sign in with new G Suite accounts in the Shared device mode >>

MaaS360 adds support for Android Enterprise Shared device sign-in with a new G Suite user account. When a user signs into the MaaS360 app, MaaS360 now displays a Configure Google Account screen as a part of the sign-in process where users can create a new G Suite account. After the sign-in, the new G Suite account is synced to the Google Admin portal.

Defect Fixes

Defect	Summary
43052	Users could not enable data roaming on the device even though data roaming was allowed in Security policies.

Android 7.50 Release Summary

MaaS360 makes the Android app version 7.50 beta available on Play Store on 24 June 2021.

ADAL to MSAL migration >>

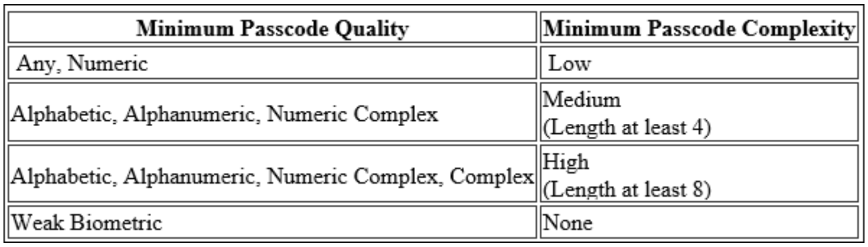
Starting with MaaS360 Android version 7.50, support for the new Microsoft Authentication Library (MSAL) will replace the Active Directory Authentication Library (ADAL). This will provide a more secure and enhanced single sign-on experience with Exchange Online, SharePoint, and OneDrive services from the MaaS360 Mail App. In order to enable authentication to Office 365 services (Exchange Online, OneDrive for Business) from the MaaS360 App (Mail, Docs) after users upgrade to the 7.50 version, changes to the Azure AD App Registration are required.

Additional behavior changes when MaaS360 targets Android 11 APIs >>

In the second phase of the series of enhancements, when MaaS360 targets Android 11 APIs on MaaS360 for Android app 7.50, there will be an impact on the Device Admin bulk enrollment feature, docs distribution feature, and changes for Files, Media, and Location permissions. **Note**: Requires MaaS360 for Android app 7.50 or later.

Passcode policy changes for Work Profile on Android 12 or later >>

Effective Android 12, Profile Owner (PO) devices require a passcode to be set in terms of complexity. MaaS360 adds a new policy setting **Minimum Passcode Complexity** that can be used to set device-wide and Work profile password restrictions in the form of predefined complexity buckets (High, Medium, Low, and None). When the devices upgrade to Android 12, a new **Minimum Passcode Complexity** setting will be applied to the devices based on the existing **Minimum Passcode Quality** setting configured in the portal.



Minimum Passcode Quality	Minimum Passcode Complexity
Any, Numeric	Low
Alphabetic, Alphanumeric, Numeric Complex	Medium (Length at least 4)
Alphabetic, Alphanumeric, Numeric Complex, Complex	High (Length at least 8)
Weak Biometric	None

Note: The default value is **Low**. Administrators can continue to use the Minimum Passcode Quality policy setting to apply password restrictions to the Android Profile Owner devices 11 or earlier.

Enhanced SafetyNet attestation to comply with the Android compatibility guidelines >>

In the previous releases, MaaS360 implemented SafetyNet Attestation API, an anti-abuse API that validates whether the device the MaaS360 for Android app is installed on satisfies the Android compatibility tests. By default, a stricter verdict of device integrity was enabled in the background (the attestation strictness was set to High). In this release, as per the guidelines and requirements of Google, MaaS360 adds a new device enrollment setting **Attestation Strictness** that allows administrators to set the device attestation strictness to High or Moderate. When set to **High**, MaaS360 evaluates whether the device passed Android compatibility tests required to be qualified as a Google-certified Android device. When set to **Moderate**, MaaS360 checks whether the device is tampered with or compromised without performing any Android compatibility tests. For example, rooted devices will fail this test.

Administrators can enable hardware-based attestation to enable the use of hardware-based security features (e.g. hardware-backed key attestation) to influence the evaluation for device compatibility.

Enhancements to the certificate pinning feature >>

Certificate pinning is a security technique that is designed to secure the communications between the client app and the server from man-in-the-middle (MITM) attacks. With certificate pinning, any attempts to establish a connection by a server to a client app with untrusted certificates will be terminated. Effective 10.82, certificate pinning will be enabled at the customer level through the MaaS360 portal Settings page. In the previous releases, it was enabled through Persona policies and applied to the devices via groups. The MaaS360 app validates the server certificate as a part of communication to MaaS360 servers, including enrollment. If an insecure network connection is detected, MaaS360 displays the Untrusted connection error message and then terminates the enrollment process. **Note**: Customers must reach out to the MaaS360 Support team for enabling the new cert pinning feature. After enabling, administrators can view the new **Validate Server Certificate** setting in the Setup > Settings > Device Enrollment Settings > Advanced > Validate Server Certificate. However, administrators cannot control (enable or disable) this setting in this release.

Data Usage renamed to Expense >>

MaaS360 renames the **Data Usage** label to **Expense** in the MaaS360 for Android app to provide a consistent user experience across all platforms.

New restriction to control location services on Android 11+ Device Owner devices >>

MaaS360 adds a new policy **Enable Location on device** to allow administrators to remotely control location services on Android Enterprise devices. However, users can manually turn the location service On or Off from the location settings after the policy is applied. **Note**: Requires MaaS360 for Android app 7.50 or later. Applicable only to Android 11+ devices that are enrolled in Device Owner mode. The default value is **Don't Set**.

Android SDK 7.50 Release Summary

MaaS360 makes Android SDK version 7.50 available on 07 June 2021.

MaaS360 adds the following changes:

Added the following method to view .EML and .MSG files in the MaaS360 Secure Mail app.

- `public static boolean viewEmailTypeDocument(Context context, Uri documentUri) throws MaaS360SDKNotActivatedException`

Android 7.41 Release Summary

MaaS360 makes the Android app version 7.41 beta available on the Play Store on 29 April 2021.

Defect Fixes

Defect	Summary
42666	Users could not reset container password through the Forgot Password workflow on Android 7 or lower versions.
42609	MaaS360 for Android app crashed during the token-based Device Owner enrollment.
42584	When users opened a link in the Secure Mail, an error message was displayed instead of redirecting to the specified app on Android 11 devices.
41650	The MaaS360 for Android app crashed after the Device Owner enrollment.

Android 7.40 Release Summary

MaaS360 makes the Android app version 7.40 available on Play Store on 16-April-2021

Display security alert on opening attachments in external emails >>

MaaS360 adds a new policy **Warn about attachments in emails from external domains** to allow administrators to configure a security alert for attachments in external emails. When enabled, MaaS360 displays a security alert on opening attachments to protect users from unintentionally opening attachments in emails that originate from external domains.

Behavior changes when MaaS360 targets Android 11 >>

When the MaaS360 for Android app targets Android 11 APIs, MaaS360 can no longer access the entire external storage directories on the device. The access is limited to specific directories and specific types of media that is supported by those directories. This means that administrators can distribute files only to the selected directories through Persona policies. While importing files into Docs and PIM apps, MaaS360 no longer displays the custom File Explorer option. However, users can use the system Files option that provides similar functionality as custom File Explorer. Users need not have to explicitly grant storage access to MaaS360 before accessing files in the Secure Viewer and Editor on Android 11 and lower versions.

Custom command support >>

Administrators can now issue custom commands to execute remote actions on the managed Android devices. After the specified action is executed on the device, the execution status can be tracked in the device history. **Note**: Requires MaaS360 for Android app version 7.40 or later.

Work Profile on Corporate Owned (WPCO) enhancements >>

In the previous releases, MaaS360 added support for *Work Profile on Corporate Owned (WPCO),* the new Android Enterprise management scenario that offers strict separation between work and personal profiles on corporate-owned devices. Effective 10.81, in addition to QR code enrollment, MaaS360 adds Zero-Touch enrollment option to set up a work profile on company-owned devices and extends WPCO support to the Samsung devices. Administrators can also enforce a new restriction **Configure personal apps to be Blocked/Allowed** to allow/block the installation of specific apps via Google Play Store in the personal profile of a company-owned device.

Granular status and error reporting for apps marked for instant install >>

MaaS360 makes it easier for the administrators to troubleshoot issues with instant install apps by adding new granular app installation statuses and retry logic. With this support, the instant install apps will report accurate app failure status (Failed instead of Pending) and device state (Out of Compliance or Selective Wipe). The status can be tracked in real-time and in case of installation/upgrade failure, MaaS360 automatically retries app installation up to 3 times on OEM devices. **Note**: Requires MaaS360 for Android app 7.40. Supported on both Device Admin and Android Enterprise devices.

Switch to a strict scheduler to schedule background tasks >>

AlarmManager and JobScheduler are among the popular methods supported in Android to schedule recurring background tasks. In the previous releases, MaaS360 used JobScheduler by default to report device heartbeat to the MaaS360 portal. In 10.81, MaaS360 adds a new policy setting: **Use Strict Scheduler for Heartbeat** to allow administrators to switch to AlarmManager, a stricter scheduler to execute background tasks such as device heartbeat. AlarmManager is strict in that the job is executed at the scheduled time even though the device is inactive, resulting in a battery drain. JobScheduler is optimized by the operating system to perform tasks when the device is charging, idle, or connected to a network.

Status of the System apps reported to the MaaS360 portal >>

If the System apps are distributed to the devices via App Catalog, the status of those apps is reported to the MaaS360 portal and displayed on the Device Summary > App Distributions page.

Conditional access to Microsoft approved client apps >>

MaaS360 adds support for conditional access to Microsoft-approved cloud apps based on the compliance status of the devices. To leverage Conditional Access, MaaS360 uses the Microsoft Authenticator broker app to register devices in Azure Active Directory. After the registration, the device compliance status is forwarded from MaaS360 to Azure AD where conditional access makes decisions to grant or deny access to the Microsoft cloud apps.

Note:

- This feature is not available by default. Contact the MaaS360 customer support team to enable this feature for your account.
- Supported only for MaaS360 Docs and Secure Viewer apps. Secure Editor and PIM are in the beta phase. Customers can try the Azure AD Conditional Access feature on PIM and Secure Editor with caution.

Resources:

- MaaS360 app registration - https://www.ibm.com/docs/en/maas360?topic=authentication-registering-your-app-in-azure-ad-tenant
- Integrating MaaS360 with Microsoft - https://www.ibm.com/support/pages/node/6433499
- Configuring cert-based authentication - https://www.ibm.com/support/pages/node/6437393
- Device registration steps Android - https://www.ibm.com/support/pages/node/6437477

Defect Fixes

Defect	Summary
42359	Fixed an Open SSL security vulnerability.
42166	When the MaaS360 Settings > Privacy tab was opened, a blank page was displayed for Android Enterprise devices.
41936	An enterprise app wrapped with MaaS360 SDK crashed on Android 11 devices.
41918	Work Profile on Corporate Owned (WPCO) enrollments through Zero-Touch configuration failed.
41680	The notification badges were not displayed on the MaaS360 for Android app in Kiosk mode.
41664	The Power button was enabled when the Kiosk mode was activated after the user manually exits the Kiosk mode.
41640, 41600	The status of the System apps was either not reported or reported incorrectly to the MaaS360 portal.
41635	The scheduled heartbeat communications failed and the devices stopped reporting to the MaaS360 portal.

Android SDK 7.39 Release Summary

MaaS360 makes Android SDK version 7.39 available on 10 March 2021.

MaaS360 adds the following changes:

- Added query tags that customers must add to the manifest file if their apps target Android 11.

MaaS360 Android Remote Support 7.35 Release Summary

MaaS360 makes the Android app version 7.35 beta available on Play Store on 27 January 2021.

Defect Fixes

Defect	Summary
41818	After TLS 1.1 deprecation, some of the older Android devices (mostly OS version 5.0) could not communicate with the MaaS360 portal for remote assistance. In the new update, MaaS360 revamps the network layer of the MaaS360 Remote Support app to support remote sessions on older Android devices.

macOS Release Summaries

MaaS360 macOS App Release Summaries

macOS 2.45.000 Agent and App Catalog 1.55.000 Release Summary

MaaS360 makes macOS 2.45.000 Agent and App Catalog 1.55.000 available on 22 December 2021.

This release includes the following enhancements and fixes:

- Certificate pinning 2.1
- Support for M1 Silicon Mac
- Other minor fixes & enhancements

macOS Agent 2.43.100, App Catalog 1.54.000, and App Packager 1.44.000 Release Summary

MaaS360 makes macOS agent 2.43.100, App Catalog - 1.54.000, and App Packager - 1.44.000 available on 06-October-2021.

Certificate pinning support for macOS >>

MaaS360 now extends cert pinning support to macOS devices. With this support, the MaaS360 app validates the server certificate as a part of communication to MaaS360 servers, including enrollment. If an insecure network connection or proxy is detected on the device, MaaS360 displays the Untrusted connection error message and then terminates the enrollment or stops the apps such as MacOS agent, App Catalog, or App Packager from functioning.

Note: Customers must reach out to the MaaS360 Support team for enabling the new cert pinning feature. Requires macOS agent app version 2.43.100, App Catalog version 1.54.000, and App Packager version 1.44.000.

Defect Fixes

Defect	Summary
42450	MaaS360 App Catalog remains in the **Loading** status on macOS devices.
1912	Fix for minimum macOS version check during App Installation.

macOS Agent 2.43.000 Release Summary

MaaS360 makes macOS Agent 2.43.000 available on 21-July-2021.

MaaS360 makes the **Escrow FileVault Recovery Key** feature generally available for all customers. This feature allows administrators to retrieve a personal recovery key on a previously encrypted device. For more information, see https://www.ibm.com/docs/en/maas360?topic=actions-filevault-disk-encryption

macOS Agent 2.42.000 and Packager 1.43.200

MaaS360 makes macOS Agent 2.42.000 and Packager 1.43.200 available on April 27.

macOS Agent 2.42.000

- Fix to upgrade Macs running macOS Catalina to macOS Big Sur.
- Fix for Uninstall-MaaS360 crash on Big Sur devices.
- Hardware Inventory data reporting correction fix.

Packager 1.43.200

- Fix for the Notarization issue with the latest Xcode.

Cloud Extender Release Summaries

MaaS360 Cloud Extender Release Summaries

Cloud Extender 2.105.300 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/6479935

Affected Product(s)	Version(s)
IBM MaaS360 Base Module	2.104.000 and prior
IBM MaaS360 VPN Module	2.102.000 and prior
IBM MaaS360 Certificate Integration Module	2.104.000 and prior
IBM MaaS360 Cloud Extender Agent	2.103.000.051 and prior

To Upgrade Cloud Extender Agent and MEG/VPN Modules

- MEG/VPN: IBM Documentation Page
- Cloud Extender agent v2.105.300.005: IBM Documentation Page

Cloud Extender 2.105.200 Release Summary

The following features/enhancements were added in this release:

- **General availability of Mobile Enterprise Gateway (MEG) support for Apple WKWebView**
  For more information, see https://www.ibm.com/docs/en/maas360?topic=module-mobile-enterprise-gateway-meg-support-apple-wkwebview.
- **MEG support for Apple WKWebView in direct mode without a load balancer**
  Administrators can configure MEG to support Apple WKWebView in direct mode without a load balancer. For more information, see https://www.ibm.com/docs/en/maas360?topic=megmsaw-enabling-mobile-enterprise-gateway-meg-support-apple-wkwebview.
- **MEG support for Apple WKWebView in High availability (HA) mode with a load balancer and TLS**
  Administrators can configure MEG to support Apple WKWebView in HA mode with a load balancer and TLS. For more information, see https://www.ibm.com/docs/en/maas360?topic=megmsaw-enabling-mobile-enterprise-gateway-meg-support-apple-wkwebview.
- **Support for Routing gateway traffic through internal proxy**

Cloud Extender 2.104.x Release Summary

The following features/enhancements were added in this release:

New DigiCert certificates added to the Cloud Extender installer to support Akamai's Kona Technology

For more information about additional MaaS360 platform updates for Akamai's Kona Technology, see the following IBM Support articles:

- - https://www.ibm.com/support/pages/node/6347900
  - https://www.ibm.com/support/pages/node/1283566

Refactored code for modernization to improve unit testing

Refactored code in the User Authentication, AD User Visibility, and LDAP User Visibility modules to improve unit testing of the modules.

Cloud Extender 2.105.100 Release Summary

Rolled back code to Cloud Extender 2.102.x

In this release, the Cloud Extender code was rolled back to Cloud Extender 2.102.x to address an issue with the AD User Visibility and LDAP User Visibility modules.