10.76 Release Summary

iOS/macOS MDM

iOS 13 restrictions support >>

To continue support for iOS 13 restrictions support, more restrictions are added under **Supervised Settings** > **Restrictions & Network** such as **Allow Network Drives Access Files App**, **Allow USB Drive Access Files App**, **Allow Find My iPhone**, **Allow Find My Friends**, **Force Wifi On**, and **Allow Quick Path Keyboard**. All these restrictions are supported on iOS 13+ supervised devices only.

Note: In iOS 13+ devices, the **Find My Friends** and allow **Find My iPhone** is combined to **Find My App** and the behavior is as follows.

- If Allow **Find My iPhone** is disabled in restrictions, then devices tab in Find My App would be disabled.
- If Allow **Find My Friends** is disabled in restrictions, then people tab in Find My App would be disabled.

New iOS policy parameters in the ActiveSync payload >>

Apple introduced flexibility in the ActiveSync payload to enable or disable individual services in the native mail app such as Email, Calendar, Contacts, Tasks, and Reminder. MaaS360 adds the support for this feature under ActiveSync payload in the iOS MDM policy. For ActiveSync payload to be set up, at least one of these services (Email, Calendar, Contacts, Tasks, and Reminder) needs to be enabled. In addition, the administrator can decide to provide the override option for users to enable these individual services. In the device, the default value set by the OS is “ 'Service' Enabled and Override Allowed” where the 'Service' can be any of these 5 services. By setting values for all 5 services in the policy, reloading of the Active-sync payload can be avoided.

If you already have ActiveSync payload that is configured and distributed, read the following instructions carefully.

1. Currently, all these five services are enabled in the native mail by default. When a new policy is created, these services are enabled by default in the policy as well to match the device's default behavior. Administrator can disable the service if needed.
2. For existing policies that has ActiveSync payload set up already, these 5 services are disabled in the policy though it is enabled on the device. When administrator makes any changes in the policy and publishes (not just in ActiveSync payload), administrator is prompted to enable at least one service. Administrator must go through the list and enable the services that are required for (or already used by) users.

In addition, MaaS360 adds two more attributes to configure OAuth authentication. **OAuth Sign in URL**-The URL that the native mail strikes to authenticate the user. **OAuth Token Request URL**- To request for the token after authentication. These settings need to be set if **Enable OAuth Authentication** is enabled. These settings are available from iOS 13+ devices.

Skip setup of items in the DEP profile configuration >>

MaaS360 adds following options in Skip Items during Device Enrollment Program (DEP) Profile configuration for iOS devices.

Welcome - If enabled, skips the Welcome screen configuration during the DEP profile setup.

Device to Device Migration - If enabled, skips the quick start configuration during DEP profile setup.

Support to automatically upload B2B apps by using VPP token >>
To support Apple's Custom B2B app workflow from Apple Connect portal, MaaS360 adds capabilities to automatically upload private (B2B apps) by using the VPP token. Enable Add Apps Automatically in the VPP token upload workflow. The function allows to automatically upload all the private apps along with the iTunes apps that are associated with the VPP token to the App Catalog. The workflow drives focus on adding private apps through VPP token for enterprise app distribution rather than traditional ipa file form to upload apps. However, when a new update is available for an app in the B2B app store, the app is not automatically updated and the support for this workflow will be available in the future releases.

Android

Enterprise app management made easier with Managed Google Play iFrame (newer version) >>

MaaS360 enhances administrative experience for customers looking to publish applications to Android Enterprise devices using a newer version of Google's Managed Play Store iframe. In the new version, administrators can browse and publish apps in a simplified and secure manner by directly uploading them to Managed Google Play Store. With this feature, MaaS360 makes Managed Google Play the single source of applications for Android Enterprise deployments for all use cases- Device Owner (DO), Profile Owner (PO) and Corporate-Owned, Single-Use (COSU). The option to add public apps via the regular Google Play Store (retail), which was redundant, has also been removed for Android Enterprise customers. There will not be any impact to apps added using regular Google Play Store option.

In the previous releases, MaaS360 displayed options to publish public apps via Managed Google Play Store or regular Google Play Store. Effective 10.76, Android Enterprise customers will publish apps via Managed Google Play Store and non-Android Enterprise customers will continue to publish apps via regular Google Play Store.

Note: The change will impact only Android Enterprise customers. Some features in iframe 1.0 have been deprecated by Google such as ability to auto-accept new permissions for future app versions and receive email notifications when there are permission changes. As a result, administrators must accept the new permissions from App Catalog manually.

Publish private and web apps directly from Managed Google Play Store >>

MaaS360 has now extended support for publishing private apps and web apps using Managed Google Play iframe. The web apps are now distributed to the devices as regular native Android apps. With this support, administrators can publish private LOB (Line-Of-Business) apps directly from MaaS360 without having to switch to Google Play Developer console.

When a private app is published,

- Google creates a Play Console account on behalf of your enterprise and waives the $25 USD registration fee.
- The app is automatically approved for your organization.
- The app is ready for distribution in approximately 10 minutes.

See **What to do next** section in the following page to understand how the feature impacts the existing private apps that were uploaded through old workflow.

https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/pag_source/tasks/pag_apps_add_private_channel.htm

Note: The **Auto-Import Android Enterprise approved apps** setting can be turned on for app updates for older apps.

Enhancements to Kiosk notification badge count >>

In the previous releases, MaaS360 added notification badge support for third-party apps deployed in traditional kiosk mode or Android Enterprise COSU mode. This feature provided ability for users to subscribe to badge notifications such as missed calls or new email alerts for critical applications when using kiosk mode, especially when notification bar was disabled.

In order to support unmanned usecases, where devices may not have a user to turn on such notifications, MaaS360 also adds a new Kiosk/COSU policy **Show App Badges** to allow the administrators to restrict the display of Show/Hide app badges option in kiosk settings on the device. This policy is turned ON by default. When the policy is OFF, the **Show App Badges** option in Kiosk/COSU settings is unavailable to the end-users.

Lock screen management policies support for devices enrolled in Profile Owner (PO) mode >>

MaaS360 extends keyguard management policies to Profile Owner (Work Profile) devices. In the previous releases, these policies were only applied to Device Owner (DO) devices.

Note: Supported on Android 9 and later devices.

New policy to allow or disable the use of Airplane mode on Bluebird devices >>

MaaS360 extends the **Allow Airplane Mode** policy to Bluebird devices that are enrolled in Device Administrator mode. This policy allows administrators to remotely enable or disable the use of Airplane mode on devices.

Path: Android MDM policy > Device Settings > Restrictions >Network Settings > Allow Airplane Mode.

Note: Requires MaaS360 for Bluebird app version 6.90.

Enhancements to app configuration settings >>

MaaS360 redesigns the app configuration settings workflow for Android Enterprise while adding support to track app configuration status at device level. The app configuration settings now support four-level nesting and hierarchical display as opposed to flat model displayed in previous releases. MaaS360 adds a new device-level action **Enable App Config Status**, allowing the administrators to track the status of managed configurations at the device level. After administrators push the configurations to the app, MaaS360 attempts to apply the configurations and retrieves the keyed app configuration state indicating its status (for example, a confirmation message or error notification). Administrators can use the device-level action **Disable App Config Status** to stop the tracking of app configuration status on the device.

Note: MaaS360 supports tracking of app configuration status only for the apps that support app feedback such as for OEMConfig apps. In order to enable app configuration status tracking, contact your IBM Account Manager for MaaS360 or IBM MaaS360 Support.

Announcement: Expect changes around Device Enrollment Mode in Device Summary for Android Enterprise devices

Until now, within IBM MaaS360 portal, for Android Enterprise use cases, both the attributes **Enrollment Mode** and **Container Type** on Device

Summary page were showing up as **Device Owner** and **Profile Owner** for DO and PO deployments respectively. These values clearly represent the type of container deployed on these devices and do not pertain to mode of enrollment.

Going forward, **Enrollment mode** attribute will start reporting actual enrollment mode for devices where the mode is available/known to MaaS360 app. Hence, **Container type** attribute shall be used in Device Summary page and in Advanced Search workflow to filter Device Owner and Profile Owner devices using *Hardware Inventory* > *Container Type* selection.

In **Devices** > **Groups** workflow, or within the custom watch list in the home page, customers who are currently using **Device Enrollment Mode** to track and group Device Owner and Profile Owner devices are requested to move to use **Container Type** attribute to filter container type on the device in order to ensure that any policy/rule assignments and application/document distributions remain intact.

In order to start tracking accurate device enrollment modes, going forward re-generate QR code and Zero Touch JSON profiles at least once and use MaaS360 for Android 6.90+.

In the next release, i.e., 10.77 Portal release, MaaS360 will be rolling out the change to read the right value for **Enrollment Mode** as **QR Code**, **Google Zero Touch**, **Knox Mobile Enrollment**, **NFC** or **DPC Identifier** (for AFW#) where information is available at the client side.

Impact after 10.77 Portal release

- Customers using **Device Enrollment Mode** attribute in device groups or home page watch lists are requested to change the attribute filter criteria to **Container Type** instead of **Device Enrollment Mode**.
- For devices running MaaS360 for Android versions below 6.90, and where administrators have not re-generated QR code or ZT JSON profiles, the enrollment mode isn't available already, so the device summary and smart search will show **Device Enrollment Mode** attribute value as Not Available.
- We are also fixing the behavior on legacy Device admin enrollments, where Enrollment Mode was always Manual. You will start to see Android Configurator where applicable. We will be introducing Container Type attribute for Device Admin devices which will read any one among following values - Device Administrator, Samsung Device Administrator, Honeywell Device Administrator, Bluebird Device Administrator, etc, where OEM SDK is integrated.

App Management

Set up auto-update of iOS apps at app level >>

MaaS360 revamps the app settings with granular auto-update settings to allow the administrators to control how apps receive automatic updates. With this support, administrators can configure whether automatic updates are controlled by the administrators or end-users, or completely disable automatic updates so that end-users manually install app updates on the device.

MaaS360 addressed the following issues with the old design:

- The auto-update settings automatically applied to all apps, so there was no way for administrators to test updates on selected apps.
- The devices did not receive the update due to user catalog preferences even though administrators enabled auto-update.

Note:

- Supported only for MDM and mixed mode customers. Not supported for departmentalized and SPS customers.
- This feature is available to new customers by default and existing customers will see the old settings.
- Supported for iTunes and Enterprise apps.

Platform

MaaS360 portal user interface enhancements >>

MaaS360 continues to enhance the user experience by revamping the application portal with new color themes and fonts. There will be further more UI changes to the MaaS360 portal in the upcoming months. In this release, there are no functional changes to the portal workflows with these UI enhancements.

User password management enhancements >>

1. **Ability to reset local user password by using URL >>** This workflow provides users with an ability to reset password without the need for administrator intervention. On the click of **Reset Password** in the User Directory, an email that contains user password reset link is sent to user's email ID. This link is active for 24 hours from the time the link is generated. Whenever a new link is generated, the old reset password link becomes invalid. **Note**: In any scenario where the user is required to enter password for validation and if expired password is entered then, user is sent an email with the reset password link to reset the local user password by using this URL. Example: During device enrollment, if expired user password is entered for authentication, then following error message "The password for the user is expired. An email is sent with a password rest link" is displayed.
2. **Scenario if a user account is locked >>** If the user enters wrong login password for more than 5 times consecutively, then, the user account

is locked for security reasons. The user is also notified with a message that the account is locked and to contact administrator to unlock the account.
3. **Password expiry management >>** A new column 'password expiry date' is introduced in the User Directory page. The column displays the date at which a user's password is set to expire. This column can be filtered based on password expiry values such as expired, expiring in 1 week, and expiring in 2 weeks.

Note: The user **Password Expiry Date** is set to 90 days from the last time the user changed the password. An email alert is sent to users to remind about password expiry at intervals of 30, 15, 7, 3, 2, and 1 day. This email includes a link that can be used to reset user password.

The Password Expiry Date attribute is also added in the End User Portal under **My Profile** page that displays the date at which the user password is set to expire.

Auto provisioning Web Services >>

MaaS360 introduces an option Manage Access Keys under **Setup** > **Web Services API**. The function allows customers and partners to generate access key without customer support intervention. With this access key management, generating OAuth token for using web services is self-serviceable. Note that only customers and partners with the access right **Web Service-Access Keys** gets an option to manage access keys. Administrator can enable this access right to the customer and partner account from the **Setup** > **Roles** page. Enable this access right to the role name for which you want to provide permission to manage access keys. This workflow can be used to generate only platform-specific access keys. The workflow is not for applicable for generating web service access keys for CISCO ISE integration (contact MaaS360 customer support) and app SDK access keys.

In this release, generate access key action and a page to view all access keys is available. In the upcoming releases, actions to deactivate existing keys and other additional capabilities will be added.

Azure multi-factor authentication (MFA) support to enroll users into MaaS360 >>

MaaS360 now supports Azure multi-factor authentication to enroll users of all devices (iOS, Android, Windows) into MaaS360.

In previous releases, MaaS360 only supported a single type of enrollment workflow where MaaS360 automatically authenticated a user by using the user's username and password credentials to enroll users into the MaaS360 Portal without user intervention.

For this release, MaaS360 also supports Azure multi-factor authentication for the enrollment workflow. The user is directed to an external Microsoft Login page to enter their username/password credential where authentication is validated by Azure, and the user is then redirected back to MaaS360 to continue enrolling into MaaS360. This feature requires that a new customer property is enabled in the MaaS360 Portal. To enable this feature, contact IBM Support.

Change To Email Address For Communications From Portal - MaaS360 will be changing the email address for the communications that originate from the MaaS360 portal. This impacts direct MaaS360 clients and does not affect the emails coming from partner accounts.

Windows

Updates to Windows-based patch management >>

For customers who signed up for MaaS360 after July 2019, and customers whose BigFix based patch management part after the July 2019 BigFix divestiture could no longer be renewed (Advanced Desktop/Laptop management), MaaS360 now provides a way to natively find missing patches and report on patches which are relevant for managed Windows (Win7 - Win10) devices and to distribute and install those patches in a granular fashion (single device or all devices). The patch management feature is available at no additional charge to all customers who have a valid MaaS360 entitlement for Windows.

CMT Co-existence and migration: Applications migration from SCCM into MaaS360 >>

As part of the SCCM Co-existence and migration capability, MaaS360's migration tool set now includes a workflow to migrate applications from an SCCM server directly into MaaS360. The CMT Migration Tool provides a new option named 'Applications Migration' in addition to GPO migration and when selected, asks for the SCCM server location and other details including login credentials. Upon submit, the tool connects to the SCCM server, fetches the metadata of the MSI applications uploaded to the server, and displays those application names in a sequence of rows in the CMT Migration Tool. The administrator can choose which applications to migrate into MaaS360, where the tool fetches all the binaries and libraries for the selected applications from the SCCM server and then uploads those applications to the MaaS360 server.

Note: For this release, only the migration of MSI apps is supported. Support for additional app types is expected in future releases.

Updates to Intune MAM integration policies in the MaaS360 Portal >>

The Intune policy workflow in the MaaS360 Portal was updated to synchronize with Intune policy additions and changes in the Microsoft Azure Portal.

Analytics

General availability (GA) of Basic Apps Inventory reports >>

From 10.76 release, Basic Apps Inventory reports are available to all customers. The Basic Apps Inventory reports show **Overview** and **Trends** statistics for the managed and non-managed apps on devices that are enrolled in the MaaS360 customer account. This report is accessible from the MaaS360 Portal at **Reports** > **Mobile Apps** > **Apps Inventory**. Subscriptions that are created in the old App Inventory report continue to receive the emails. The migration of these subscriptions to the new report will be done at a later date. Customers can subscribe to the new reports from the **MaaS360 portal** > **Setup** > **Settings** > **Administrator Settings** > **Analytics**.

10.75 Release Summary

iOS/macOS MDM

Configure Office365 Endpoint URL in the Persona Policy settings >>

MaaS360 includes Office365 Endpoint URL in the Persona Policy under Email Advanced settings. On enabling the SSO during secure mail configuration, you see the option to enter the Office365 Endpoint URL. The default endpoint URL for Office365 is https://outlook.office365.com. When this URL is changed, MaaS360 email app will hit the configured URL instead of default URL when launched. This setting is supported on iOS 3.95+, Android App 6.70+ devices only.

DEP Profile configuration UI updates >>

Few of the DEP profile attributes are deprecated by Apple and the same is changed in MaaS360 as well.

Require MDM Enrollment - Irrespective of the value selected here, the device will always enroll to the MDM server if it has internet connection during bootup.

Supervise Device - Any new DEP device enrolled will become a Supervised device by default. The value in this attribute will not be respected going forward.

Allow Host Pairing - This attribute from DEP profile is removed. Customers can use the Allow Pairing option in the MDM policy instead.

iOS 13 restrictions-Zero Day Support >>

Apple has deprecated few of the restrictions for managed devices and added them to restrictions for Supervised devices. We have added them under **Supervised Settings** > **Restrictions & Network.** We still have existing restrictions under managed section in the policy, but will not be respected by devices from iOS 13.

Android

Device Administrator (DA) to Work Profile migration >>

Users can now enable the Android Enterprise Work Profile migration (also called Profile Owner) for bring your own devices (BYOD) that are enrolled as a Device Administrator. To enable this feature in the MaaS360 Portal, go to Settings > Enrollment Settings. Follow the setup instructions in Migrating from Device Admin (DA) to the Work Profile before you migrate devices.

Advanced Android Enterprise policies on restrictions and Kiosk mode/corporate owned single use (COSU) settings

MaaS360 adds advanced policies on restrictions and Kiosk mode/corporate owned single use (COSU) settings for Android Enterprise devices. For more information, see https://www.ibm.com/support/pages/node/1073746.

New commands when device is in direct boot mode

Administrators can now issue commands such as device wipe, reset passcode, and profile wipe when a device is in direct boot mode. For more information, see https://www.ibm.com/support/pages/node/1073840.

Changes to the download URL for Samsung Knox Mobile Enrollment (KME) and Android Enterprise Zero-touch enrollment setup

MaaS360 replaces the version-specific agent download URL for Samsung Knox Mobile Enrollment (KME) and Android Enterprise Zero-touch enrollment setup with a generic URL that points customers to the latest version of the MaaS360 app. Customers who create profiles for KME or zero-touch enrollment receive the most current version of the MaaS360 app automatically, and no longer need to manually update their enrollment profiles.

Android 6.80+ release summary

The Android 6.80+ release includes the following features and improvements for the MaaS360 Android agent app and for Android devices that are enrolled in the MaaS360 Portal:

- The MaaS360 core app is exempt from battery optimization by default. The app will not enter battery saving mode on the device even if the user has not accessed the app for a long period of time.

- MaaS360 uses a new API from Samsung that resets the password on Samsung Knox 3.2.1+ devices that are enrolled in Device Admin mode.
- For WorkPlace authentication on Samsung devices, MaaS360 now supports iris and facial recognition, in addition to supporting fingerprint scans. For more information, see https://www.ibm.com/support/pages/node/1073748.
- For apps in Kiosk mode, MaaS360 displays notification badges that inform users about missed calls or unread email messages. The Kiosk launcher Settings (gear) icon was redesigned to appear more prominently on any device background. For more information, see https://www.ibm.com/support/pages/node/1073822.
- When the MaaS360 for Android app enters background mode during device enrollment, enrollment screens that contain confidential information are not displayed until the user accesses the device. Users are also prevented from taking screenshots of enrollment screens.

App management

Deep links support for installing apps on an Android agent >>

With MaaS360 for Android 6.80+, administrators can create deep links that allow users to install Google Play or Private apps on Android Enterprise (DO or PO) devices. With this support, users can bypass the App Catalog and install apps by tapping on the deep link that is sent from the administrator.

Note: The app must be available in the end-user App Catalog. The deep link must contain all the necessary parameters. The device must be enrolled in DO or PO modes.

Windows

Group Policy Migration Tool enhancements: New HTML Summary report for Group Policy Objects (GPO) policies to MDM policy migration >>

The Group Policy Migration Tool now displays a View Migration Summary button that allows you to generate an HTML report that summarizes the GPO policies that were migrated to an MDM policy. The report also summarizes the GPO policies that were not migrated because MaaS360 or the MDM does not support those policies.

New CMT Migration Status column in the MaaS360 Portal Device Inventory view shows the status of co-managed devices >>

The Device Inventory view in the MaaS360 Portal now provides a new customizable column called CMT Migration Status. The CMT Migration Status column displays the following values for migrated devices:

- Co-existing with SCCM: Devices that are managed by both SCCM (Microsoft System Center Configuration Manager) and MDM.
- Migrated from SCCM: Devices that were fully migrated from SCCM and are now managed by MDM only.
- Not Applicable: Devices are not co-managed because the SCCM client was never installed on the device.

Advanced search using the new CMT Migration Status device keyword attribute >>

From the Advanced Search view in the MaaS360 Portal, you can now use the CMT Migration Status keyword attribute to search for devices that are co-managed by SCCM and MDM or fully migrated from SCCM to MDM.

Updated list of Group policies that can be migrated as MaaS360 Windows MDM policies using the Group Policy Management Tool >>

This release provides an updated version of the Group Policy Management Tool and additional support for Group policies that can be migrated to Windows MDM policies using the tool.

- The **License Entitlements** summary page for the device that shows the list of licenses that are applicable on the device along with time from the license is applied and expires is displayed.

10.74 Release Summary

iOS MDM and macOS MDM

Enhancements to Functionality macOS MDM policy

The Functionality macOS MDM policy now supports the Allow Screenshot option that restricts screen captures and screen recordings on macOS 14.4+ devices.

Android

Android Enterprise Migration Program: General Availability of DA to Work Profile migration >>

MaaS360 announces the general availability of the Device Admin (DA) to Work Profile (Android Enterprise Profile Owner) migration. For this release, MaaS360 adds support to migrate multiple devices at once (group action), enforces the Work Profile migration (forced migration after 90 days), activates Samsung Knox License (SKL) / Enterprise License Management (ELM), and tracks migration status in the Action history. **Note:** This feature requires the MaaS360 for Android agent version 6.70 and later.

Android Enterprise as the default enrollment mode

MaaS360 now allows administrators to make Android Enterprise the default enrollment mode for organizations that want to move off the Device Admin deployment mode and adopt Android Enterprise. MaaS360 also displays an alert message on the MaaS360 Portal Home page if Android Enterprise is not set up for the organization.
For new customers, Android Enterprise must be set up in the MaaS360 Portal to complete Android Enterprise enrollments on the device. Existing customers can contact their MaaS360 Account Representative to enable this feature for their account.

Configuring the minimum OS restriction for Android Enterprise self-enrollments >>

MaaS360 adds support to allow administrators to enroll Android Enterprise devices based on the minimum OS version of the device. This feature allows organizations to implement a phased adoption to Android Enterprise. The administrator can push the OS version to Android Enterprise and older OS versions can fall back on Device Admin deployment. Administrators can use the self-enrollment options in the Device Enrollment settings to configure the OS versions that are used for Android Enterprise. When users start enrolling their devices, the devices that meet the minimum OS requirement are enrolled into Android Enterprise (Work Profile) and the devices that do not meet the minimum OS requirement fall back to Device Admin deployment.

Blocking automatic system updates on Android devices >>

MaaS360 adds support to block automatic system updates during a scheduled time to allow administrators to evaluate the new update for compatibility before rolling the update out to employee devices. Administrators can suspend system updates for up to 90 days. When a device is in the freeze period, the device does not receive notifications about pending system updates, install system updates to the OS, and users cannot manually check for system updates.

MaaS360 for Android includes various behavior changes for Android OS version 10. For more information, see https://www.ibm.com/support/docview.wss?uid=ibm10957305.

New TeamViewer unattended access retry logic

When an administrator sends an unattended access request for TeamViewer Remote Support, MaaS360 tries to re-initiate remote support on the device, up to one minute. In previous releases, when the TeamViewer host app was inactive, the initial request failed to execute and MaaS360 displayed an error message without waiting for the host app to become active again.
With the new retry logic, MaaS360 sends four unattended access requests at 15 intervals each over the span of one minute to establish unattended access connection to the device.

New closed track testing for Android Enterprise apps >>

Google no longer supports the current method for managing tracks. If an administrator hovers over an existing distribution of an alpha/beta app version in the App Catalog, track information is no longer displayed for those apps. By default Google tracks all existing apps at the production versions, not the alpha/beta versions.

For the new method, administrators must whitelist their enterprise apps (alpha/beta, custom) for the track that they want to test. The MaaS360 App Catalog displays the track in the App Summary during the next app refresh. The update can take up to seven days. The administrator can also manually refresh the app, which can take up to four hours to refresh.

When the track is available in the MaaS360 App Catalog, the administrator can distribute the track by using the Distribute app workflow. MaaS360 displays an associated track ID against each track in the app distribution workflow to allow administrators to uniquely identify the app track. Administrators can also view and distribute apps to the custom closed app tracks that are created by app developers in the Managed Google Play Console.

App management

Editing the Download URL for enterprise apps for Android >>

The Download URL specifies the location where the actual .apk file is hosted. Administrators can provide a download URL when uploading an enterprise app for Android so that the app is downloaded from a specific location instead of from the MaaS360 tenant CDN. For organizations that use the local organization specific CDN location to host enterprise apps for Android, MaaS360 now adds support to edit the Download URL after the app is added to the MaaS360 Portal. This feature allows new installations to pick up the app from the updated location.

Disabling the removal of macOS apps >>

MaaS360 adds support to allow administrators to prevent users from removing the macOS iTunes App Store apps on the device. All apps that are eligible for uninstallation are displayed in the Uninstallers tab in the end-user App Catalog. For this release, MaaS360 adds a new flag `Allow Uninstaller for Users` for macOS App Catalog workflows at the app level. If this setting is disabled, the macOS app is not displayed in the Uninstallers tab in the end-user macOS App Catalog.

Enhancements to the app installation lifecycle >>

MaaS360 renames the existing app distribution status and provides an in depth view of the app installation lifecycle. The app distribution status allows administrators to track installation progress and to troubleshoot issues during app deployments. This feature is supported on iOS and Windows app deployments only. Windows devices support the `Failed` status only.

Windows

Support to install/uninstall more than one version of Office >>

MaaS360 adds support to install and uninstall more than one version of Office on the same Windows machine.

Support for co-managing devices >>

MaaS360 adds support for co-managing devices with the Microsoft System Center Configuration Manager (SCCM) and MDM. For this feature, administrators can take the following actions:

- Deploy the Bulk Provisioning Tool to endpoints through SCCM
- Migrate the Group policy
- Override the Group policy with the MDM policy if there are policy conflicts

10.73 Release Summary

iOS/macOS MDM

Manually install downloaded profile while enrolling iOS 12.2+ devices (MDM) >>

To improve platform security by reducing misleading profile installations during iOS enrollment, MaaS360 aligns with Apple's new method of manually installing the downloaded profile. From the device Settings page, you can inspect each of the downloaded profiles and install the required MaaS360 MDM enrollment profile on the device. The new method of manually installing the profile is supported on iOS 12.2+ devices. For devices before iOS 12.2 and on macOS, the enrollment method remains unaffected.

Note that for enrollment on any version of iOS or macOS devices, the user is alerted to complete the MDM profile installation before continuing to install apps.

Manually download and install MDM profile while deploying MDM to corporate devices using the Apple configurator tool >>

Bulk deploying of MDM to corporate devices by using Apple Configurator includes an additional step to download and install the MDM profile manually in the iOS 12.2+ devices before assigning the devices to the user. This step is added to support the Apple's new method of enrolling iOS 12.2+ devices (MDM).

Support for kernel extension in macOS MDM policy >>

MaaS360 adds "Kernel Extensions" setting in the Advanced settings of the macOS MDM policy. The setting allows users to whitelist kernel extensions by using team IDs and to approve the third-party kernel extensions that are not part of the policy. When no bundle ID is provided, all the kernel extensions that are associated with the team ID are white-listed. When both bundle IDs and team ID are provided, then only those bundle IDs associated with the team ID are white-listed. The setting prevents the OS from blocking these kernel extensions on macOS 10.13.2+ devices.

Support for Intercede certificate authority for Derived Credential Authentication >>

Along with Entrust and Purebred certificate authority, MaaS360 includes Intercede certificate authority to perform Derived Credential Authentication. These certificate authority options are displayed under Derived PIV Credentials Settings in the Basic **App Settings** page.

Certificate based authentication for SDK apps >>

MaaS360 allows iOS SDK apps to authenticate to server by using Identity certificate that is configured in the Basic **App Settings** page. Enable the certificate-based authentication from the **WorkPlace Apps** > **Security** in the WorkPlace Persona policy setting and choose from the configured PIV-D/CE credential certificate to be used for authenticating the iOS SDK apps.

Support for Bluetooth based authentication for Workstations >>

MaaS360 adds Bluetooth-based authentication support for Workstations. This setting is supported on iOS 10.0+ devices and applicable only if Entrust is selected as the Derived Credential Vendor. Configure this setting in the Security WorkPlace Persona policy.

Support for server logging for Siri and personal hotspot settings in iOS MDM policy

MaaS360 adds the following settings for iOS 12.2+ devices in the iOS MDM policy settings:

- **Server logging for Siri**: Accessible under device restriction settings. When enabled the setting allows siri to server-side login.
- **Allow personal hotspot modification**: Accessible under restrictions and network settings. When enabled, the setting allows user to modify personal hotspot settings on the device.

Analytics

Unified endpoint management (UEM) Overview reports for mobile devices >>

MaaS360 offers new business dashboards for Unified endpoint management (UEM) named as UEM Overview that includes mobile devices reports for all device platforms. Contact IBM MaaS360 Customer Support team to enable the UEM Overview reports for the customer account. Once enabled, the MDM Overview report is replaced with the new UEM Overview reports.

Subscription settings for these reports are listed under Analytics section in the Administrator Settings from where administrator can configure the subscription and the UI settings. Once configured, the UEM Overview reports are accessible from the Reports tab in the MaaS360 portal.

Android

Support to assign a custom device name to enrolled Android devices >>

MaaS360 now allows administrators to change the device name of the enrolled Android devices through a new device level actio . Administrators can assign a custom device name that makes it easier for them to identify the devices at a glance. Note: Supported on Android devices enrolled in both MDM and Android Enterprise.

Set default locale and timezone through QR code and Zero-touch enrollments

Some usability enhancements have been added to QR code and Zero-touch enrollment workflows that will allow administrators to set default locale and timezone on devices during enrollment. However, it is to be noted that users can change the locale and timezone on the device after the enrollment.

Support to restrict app installs to Google Play >>

On Android Enterprise devices enrolled with Work Profile (Profile Owner), it was not possible for administrators to disallow uninstallation of apps from unknown sources on the personal side.

MaaS360 adds support for new policy "Allow device wide restriction on installation of apps from Non-Google Play". This policy is applied at the device level even for devices with work profile only due to which the app installations from unknown sources can be blocked in both personal profile and work profiles.

Note: This policy is only applicable to Android 9.0 and later devices enrolled in PO mode. The system settings remain active on the device, but the system blocks app installation. This policy only affects future installations so the apps that are already installed through unknown sources remain on the device.

Support to control the maximum device enrollments allowed per user account

Recently, Google imposed a restriction on user accounts enrollment that it will support only a maximum of 10 devices per Android Enterprise user account. In accordance to this restriction, MaaS360 will show a warning message to end users in case a eleventh device is enrolled with the same user account.

There may be a chance that end users may ignore this warning message and proceed with the enrollment.

In case you want to enforce the restriction in your organization, contact MaaS360 Support who can set this configuration to "Do not allow enrollment" when more than 10 devices are enrolled with the same Android Enterprise user account.

Single sign on to G-Suite during Android Enterprise enrollment >>

MaaS360 adds cert-based authentication support for enrolling devices into Android Enterprise (G-Suite/Managed Google Account). G Suite customers leveraging IBM Cloud Identity can seamlessly authenticate the MaaS360 app during the Android Enterprise enrollment process.

In the previous releases, when IBM Cloud Identity was used as the identity provider for G-Suite, the users had to authenticate the MaaS360 app with their Cloud Directory credentials.

Note: The user certificate is removed from the device after enrollment. Requires MaaS360 for Android 6.60 agent.

Real-time update of Android Enterprise approved apps

MaaS360 takes advantage of Google EMM Notification APIs to receive application updates notification for approved apps in Managed Play Store near real-time. In the previous releases, MaaS360 relied on a batch job ran once a week to process application updates (approved/unapproved).

Note: The apps that are not updated through Google EMM Notification APIs will be continue to be updated through the batch job.

Decoupling ownership in deployment settings for Android Enterprise Device Owner Enrollment

MaaS360 adds support to discover DO mode enrollments without relying on self enrollment options in deployment settings. Previously, the QR code and Zero-Touch Device Owner enrollments failed if corresponding device ownership options were not selected in self-enrolment options in the deployment settings.

Windows

Migrating from App Compliance Settings to Advanced App Compliance Settings in Windows MDM policy >>

The Advanced App Compliance is a new policy setting introduced in 10.73 to create Blacklist(Deny)/Whitelist(Allow) of Universal and Desktops apps and binaries for Windows 10 desktop/laptop/tablet devices. It enhances existing methods of creating and maintaining the blacklist and whitelist of applications, by allowing blacklisting of applications from a publisher, excluding some apps from the publisher in the same blacklist or whitelist,

blacklist based on File Path, File Hash of the applications and so on. You can manage numerous such blacklist and whitelist entries using this new Advanced App Compliance with minimum effort.

With the introduction of this new tab, the Application Compliance tab will be deprecated and Administrators are recommended to move existing desktop/laptop based blacklist/whitelist entries from ‘App Compliance’ tab to ‘Advanced App Compliance’ tab.

Support for address based location Geo-fencing for Windows >>

MaaS360 adds support for address based Geo-fencing for Windows 10 (Enterprise and Pro) desktop, laptop, or tablets.. The geo-fencing rule, included with the compliance rule set, places a device out of compliance if a device is removed from a designated secure location. Administrators can perform actions against the device and also apply policies to the device when the device checks back in from a designated secure location.

This setting requires MES 2.16+ and MaaS360 Core App for Windows 4.0+.

Platform

Support to delete inactive devices from MaaS360 Portal >>

MaaS360 adds support for deleting inactive devices from the **Device Inventory** view. Bulk delete support will be added in a future release.

Modify Users Web services API

MaaS360 adds support to add or remove multiple users to a Group. Administrators can modify the users of group with a single API call.

Account Actions Control Access rights for Partner administrators to control the visibility of actions >>

MaaS360 introduces Access Rights for Partner administrators in the **Account Actions Control.** With the new feature, Partner admins can now restrict administrators from creating, convert, and expiring accounts but still perform Partner Role functions like **Reporting** and **Manage As**.

Administrators with the new access rights can control the visibility of the following actions present on the **Accounts** page :

- Extend
- Expire
- Rename Account
- Move
- Delete Account
- Add Account
- Convert
- Add Partner

The new access right for Accounts page will be given to "Partner Administrator" role by default. To create an admin with the "View only" access to accounts page, create a role and copy the access right present in "Partner Administrator" role excluding "Account Actions Control" access right, and assign it to the admin.

The following actions are not affected by the new access right:

- Manage As
- View
- Export

The following details will not be editable with the new access right:

Customer details

- Default Language
- Default Country
- Customer Vertical
- Committed Licenses
- Billing Start Date

The following details will not be editable with the new access right:

Partner details

- Force admins to accept EULA
- Default trial period for Customers

- Default language
- Email domain list for creating multiple accounts
- Default Country
- Type of account allowed
- Customer registration schema
- Template visibility
- Maximum duration allowed for trial accounts(days)
- Threshold for enrollment notification via email

Cloud Extender 2.97

Direct Certificate Authority access to the Microsoft Certificate Authority server >>

The Certificate Integration module now provides an alternative to the SCEP method for requesting device certificates from a Microsoft Certificate Authority server. The Cloud Extender provides a feature that directly obtains certificates from Microsoft Certificate Authority servers that reside in the same forest, or trusted forests, as the Cloud Extender server.

Push notifications through the Apple Push Notification service (APNs) >>

The Cloud Extender uses Exchange Web Services (EWS) to subscribe to notifications for user's mailboxes. MaaS360 now uses Cloud Extender to send push notifications to intended devices through the Apple Push Notification service (APNs). When you enable remote notifications, notifications are delivered to the device even if the device enters the background or is terminated.

10.72 Release Summary

iOS/macOS

SMIME configuration in iOS MDM policy setting >>

MaaS360 enhances the SMIME feature that is part of Exchange payload for iOS MDM policy. "Configure SMIME" section is introduced to have all SMIME settings under one section, which was scattered before. In addition, there are 4 more new configurations that are introduced and described below.

1. Allow user to override enabling/disable encryption - If enabled, user can choose to enable or disable encryption on the device.
2. Allow user to override S/MIME signing value - If enabled, user can choose to enable or disable signing on the device.
3. Allow user to override encryption certificate - If enabled, allows user to choose the encryption certificate to use on the device from the Advanced settings > S/MIME > "Encrypt by Default" option on the device.
4. Allow user to override SMIME signing value - If enabled, allows user to change the Signing certificate to use on the device from the Advanced settings > S/MIME > "Sign" option on the device.

Previously, the user would not be able to override the encryption and signing settings that was set by the administrator.

Enable oAuth authentication for iOS and macOS >>

MaaS360 includes "Enable OAuth authentication" setting in iOS and macOS MDM policy to allow users to use OAuth 2.0 for authentication. The setting is supported on iOS 12.0+ and macOS 10.14+ devices.

In iOS MDM policy, the setting is listed under Device Settings > ActiveSync.

In macOS MDM policy, the setting is listed under User Settings > Exchange.

When OAuth is enabled, the authentication workflow will hit the configured OAuth url in the native mail app.

New grouping mechanism for Notifications in iOS policy setting >>

With iOS 12.0+, Apple is providing new mechanism to group notifications in the device. To support this feature, MaaS360 introduces "Grouping Type" setting in the iOS MDM policy under Supervised Settings > Notifications. The settings is supported for only supervised devices.

Grouping of notifications is based on "automatic", "by app" and "off" notifications. If grouping type is set to "off", the notifications are not grouped.

The default mode for grouping notification type is "automatic".

- The "automatic" grouping is based on how individual app wants the notifications to be grouped.
- For an "App" group notification, the alerts from an app are put under a single group.

Skip setup of items during Profile configuration in Device Enrollment Program >>

MaaS360 adds following options in Skip Items during Profile configuration for iOS, macOS, and all DEP devices.These are supported from iOS 12 and macOS 10.14.

Screen Time - Skips the screen time configuration during the set up

Software Update - Skips the mandatory software update screen during the set up

Appearance for macOS - Skips the choose your look in macOS set up

Sim Set Up - Skips the add cellular pane during the set up.

Time server configuration in macOS policy setting >>

MaaS360 supports new policy setting "Timer server" in macOS MDM policy. Enable the time server configuration in the policy and specify the time server and time zone values. On publishing this policy on the macOS device, the device time is synced with the configured server time and time zone in the policy and it cannot be changed by the user on the device. This setting is supported on macOS 12.4+ devices.

App store restrictions on macOS >>

MaaS360 introduces 2 new App Compliance restriction settings in the macOS MDM policy.

Allow non admin users to install apps- If enabled, allows non-administrator users to install applications from the App store. The setting is supported on

macOS 10.9+ devices.

Allow software update notifications- If enabled, allows software update notifications. The setting is supported on macOS 10.10+ devices.

Android

Android Enterprise policies for Browser and Lock Screen on Samsung Knox devices

For Android MDM, the Browser and the Lock Screen policies use a new support tag PO with Knox and DO with Knox for the Android Enterprise settings.

-

Migration from Google Cloud Messaging (GCM) to Firebase Cloud Messaging (FCM)

Google announced the decommissioning of Google Cloud Messaging (GCM) on April 11, 2019. EMM vendors must move to Firebase Cloud Messaging (FCM) to provide real-time notifications to devices. Firebase Cloud Messaging (FCM) is a new push notification mechanism for communicating with any Android app from a web server such as EMM. MaaS360 will move to Firebase Cloud Messaging (FCM), which inherits the reliable and scalable Google Cloud Messaging (GCM) infrastructure.

Customers should upgrade to Android agent 6.50+ as early as possible. Existing devices continue to work after April 11, 2019 until a device group must be re-enrolled. For re-enrollment, administrators should consider upgrading the device first to Android agent 6.50+ and then complete the enrollment.
Note: Google Cloud Messaging (GCM) deprecation does not affect devices that are not supported by Play Services.

Migration impact

Devices that are enrolled before MaaS360 for Android app version 6.50 are already registered with Google Cloud Messaging (GCM) and continue to use Google Cloud Messaging (GCM). The Google Cloud Messaging (GCM) token continues to work indefinitely.

The devices that are enrolled with MaaS360 for Android app version 6.50 and later are registered with Firebase Cloud Messaging (FCM). The Firebase Cloud Messaging (FCM) server generates both Google Cloud Messaging (GCM) and Firebase Cloud Messaging (FCM) tokens for Google Cloud Messaging (GCM) and Firebase Cloud Messaging (FCM) registered devices. Any new enrollments with the Agent version earlier than MaaS360 for Android app version 6.50 cannot create a new Google Cloud Messaging (GCM) token, when Google deprecates support for Google Cloud Messaging (GCM) in April. Devices must upgrade to MaaS360 for Android app version 6.50 and later to re-enroll.

Beta release of the Samsung Knox License (SLK) and Knox License Management (KLM)

MaaS360 adds support for Samsung Knox License (SLK) management that allows an administrator to deploy the Samsung Knox License (SLK) key to Samsung devices.
Samsung Knox License (SLK) is a consolidated license that is designed by Samsung to replace Enterprise License Management (ELM) and Knox License Management (KLM) licenses. This feature requires MaaS360 for Android 6.50+ and Knox 3.0+.

Note: This feature is not available by default. Contact IBM Support to enable this feature for your account. The Samsung Knox License (SLK) key expiration is not handled by MaaS360 yet. If you provide a key that is about to expire, you will lock users out of the Profile Owner mode and encounter issues in Device Owner mode. When this feature is enabled, all Android Enterprise enrollments on Knox 3.0+ devices require a Samsung Knox License (SLK). If the Samsung Knox License (SLK) is not functioning properly, enrollments can fail.

Configuring the Samsung Knox License (SLK) from the Settings menu option in the MaaS360 Portal

To configure the Samsung Knox License (SLK) key from the Settings menu option in the MaaS360 Portal:

1. Go to Setup > Settings.
2. In the Device Enrollment Settings section, click Advanced.
3. Expand the Advanced Management for Android Devices section and then enter the Samsung Knox License (SLK) key.

Configuring the Samsung Knox License (SLK) from policies in the MaaS360 Portal

To configure the Samsung Knox License (SLK) key from policies in the MaaS360 Portal:

1. Go to Security > Policies.
2. Open an Android MDM policy, expand the OEM Settings section in the sidebar, and then click Samsung License Management.
3. Enter the Samsung Knox License (SLK) key and the Knox License Management (KLM) key.

Track-only mode for IBM Trusteer® Threat Management

MaaS360 adds a new remediation action that allows administrators to track malware apps only. The Track only action allows administrators to keep a track of all devices that are running malware apps, but does not immediately take action on devices to remediate the issue. The user is not notified about the malware and the device is not placed out of compliance. In previous releases, the app was uninstalled from the device or the device was placed out of compliance based on the policy setting. This setting is available from Device Settings > Trusteer Threat Management > Configure Settings > Malware App Remediation Action.

Track the Kiosk mode status on devices

MaaS360 allows administrators to easily track the stages of the Kiosk mode from the Kiosk Mode field in the Devices view. Administrators can also create advanced search criteria to filter devices in Kiosk mode by status.

To view the Kiosk mode status: Go to Devices > Inventory and then open the device. In the Device Summary view, the Kiosk mode status is tracked in the Kiosk Mode field.

The following stages are tracked in the Kiosk Mode field:

- Enabled: Kiosk mode is enabled on the device through policies.
- Pending Enablement: The Kiosk mode policy is published, but Kiosk mode is not enabled on the device.
- Exited: The Kiosk mode is enabled through policies, but the user exited the Kiosk mode.
- Not Applicable: The default value before enabling the Kiosk mode on the device is enrolled with MaaS360 for Android version 6.50 and later.
- Not Available: The default value before enabling the Kiosk mode on the device is enrolled with MaaS360 for Android version earlier than 6.50.

App wrapping support for apps compiled with the AAPT2 (Android Asset Packaging Tool)

MaaS360 now allows users to wrap apps that are compiled with AAPT2 (Android Asset Packaging Tool), a build tool that Android Studio and Android Gradle Plugin use to compile and package resources for the app.

App management

General availability of app inheritance >>

MaaS360 adds support for app inheritance that allows hierarchical management of public apps (iOS, Android, Windows, and macOS) and inheritance of these apps from channel partners to customers while controlling the apps that the customer receives. Any changes to apps at the partner level are applied to all customers and partners under the channel partner without any additional work required at each customer level. Channel partners can distribute apps or make them available to customers or partners. **Note:** The apps that are distributed by channel partners cannot be deleted by customer administrators.

Deploy web apps to macOS devices

MaaS360 now allows administrators to deploy web apps to macOS devices. The deployed web apps are available from the Web Apps section in the App Catalog agent. **Note:** By default, the web apps are opened in the Safari browser. This feature requires macOS App Catalog agent version 1.50.000.

Post-enrollment installation of an app bundle

Administrators can deploy enterprise apps that are automatically installed on macOS devices after enrollment. This feature also allows administrators to arrange bundles in the order that they are installed on the device. **Note:** This feature is not available by default. Contact IBM Support to enable this feature for your account. When the Startup Bundle is enabled, the app bundle is marked for instant install. This feature is supported on macOS enterprise apps only and requires macOS App Catalog agent version 1.50.000.

To add a post-enrollment installation bundle from the MaaS360 Portal:

1. Go to Apps > Bundles.
2. Click Add App Bundle. The App Bundle window is displayed.
3. Complete the fields, and then select the Startup Bundle check box.

To arrange the order of post-enrollment installation bundles in the MaaS360 Portal:

1. Go to Apps > Bundles.
2. Click Order Startup Bundles.
3. Drag and drop the startup bundles to arrange the order.
4. Click Save Order.

Windows

Automatically connect to wifi network in range >>

MaaS360 allows devices to automatically force connect to the Wifi network that is in range and prevents from connecting to an alternative network. The "force connect" connection mode is added in the Windows MDM policy under wifi settings. The connection mode is supported on Windows 10 MDM devices and Agent: MDM Extender 2.10.x.

Install Office 365 suite on Windows 10 devices >>

MaaS360 supports silent installation and uninstallation of Office 365 suite on Windows 10 MDM devices through a simple device group action. Using this action enables a Microsoft Office client to be installed or uninstalled on devices from the Office Deployment Tool (ODT). This action is supported on Windows 10 devices 1703+. The actions to Deploy Office 365 Suite and uninstall Office 365 suite allows administrators to attach an Office configuration XML to auto download and auto installation or remove various Office365 editions. The Office Configuration XML file is sent to the Office Deployment Tool through MDM commands to trigger the installation or uninstallation as needed.

Advantages of using Office Deployment for Office 365 installation are:

- Organizations can easily distribute Office applications by using the Office Customization tool that provides various options for bandwidth optimization that includes to use a local server as download source.
- For an organization with geographically distributed users, it is possible to distribute different language files based on user regions or OS language.
- Flexibility to install different Office products for different groups based on whether the group of users are approved to use a specific office product license or not.

Association of user name for bulk enrolled devices >>

During association of a user account to a bulk enrolled Windows 10 device, the user association process takes about 30 minutes to complete on devices. The details such as policy set, ruleset, expense plan, apps that are associated with user account and other user details are updated on the device according to the details present in the uploaded .CSV file.

Passcode and User accounts - Profile Management policies for HoloLens devices

MaaS360 provides added support to handle security for HoloLens devices, including enhanced support for the following policies in Windows MDM:

- Passcode: The Passcode settings enforce the use of a secure passcode to unlock a HoloLens device. This policy enforces passcode restrictions such as passcode length, passcode value, quality of the passcode, and the minimum amount of characters.
- User accounts - Profile Management: Administrators can delete user profiles on devices with multiple inactive users to manage storage space on devices. The following settings are now available for this policy:
  - Deletion Policy
  - Storage capacity percentage threshold to start profile deletion (%)
  - Storage capacity percentage threshold to stop profile deletion (%)

  Note: The User accounts - Profile Management policy is supported on HoloLens Business Edition only.

To enable either of these policy settings, go to Security > Policies > Windows MDM policy > Device Settings.

Geo-fencing rules to manage wifi locations for Windows devices >>

MaaS360 introduces geo-fencing support for Windows 10 desktops, laptops, and tablets. The geo-fencing rule included with the compliance ruleset places a device out of compliance if a device is removed from a designated location, including managed wifi locations. The administrator can issue actions or dynamic policies on the device to restrict the use of the device if the device is removed from a designated wifi location.

Note: Geo-fencing is currently enabled for managed wifi-based locations for Windows 10 desktops, laptops, and tablets for Pro, Education, and Enterprise editions. This setting requires MES 2.0+ and MaaS360 Core App for Windows 4.0+.

Define custom attributes from the status of a service on a Windows device

Maas360 introduces a feature to define and handle custom attributes based on the installed or running status of a service on a Windows 10 device. This setting requires Windows MES agent 2.10+. Contact IBM Support to enable this feature.

Notification - DigiCert End Of Sale notice for Symantec Enterprise Mobile Code Signing Certificate impacts Windows Phone 8.1 and Windows Phone 10 Management

DigiCert has announced that DigiCert and Microsoft will discontinue issuing the Symantec Enterprise Mobile Code-Signing Certificate after February 28, 2019. Organizations that use this certificate with MaaS360 for Windows Phone 8.1 or Windows Phone 10 management are impacted if they do not

renew the certificates prior to February 28, 2019. For more information, see https://products.websecurity.symantec.com/orders/enrollment/microsoftCert.do.

Organizations that continue to use Windows Phone 8.1 or Windows Phone 10 management with MaaS360 should consider renewing their existing Mobile Code Signing Certificate before February 28, 2019. To continue to manage existing Windows Phone devices, upload the renewed Symantec Mobile Code Signing Certificate to the MaaS360 Portal at Setup > Services before the current certificate expires. After February 28, 2019, Symantec will no longer issue certificates. Microsoft has not announced a replacement vendor for these certificates. Self-signed certificates or other vendor certificates are not valid.

Impact from not renewing the Symantec Mobile Code Signing Certificate: Windows Phone devices that are already enrolled with MaaS360 continue to work as long as the existing Symantec Enterprise Mobile Code Signing Certificate that is uploaded to MaaS360 remains valid.

If you fail to renew the Symantec Enterprise Mobile Code Signing Certificate by February 28, 2019 and upload a certificate to the MaaS360 Portal before the current certificate expires, the following services will not work on Windows Phones that already enrolled with MaaS360 or new Windows Phones that enroll after the certificate expiration date:

- MaaS360 App for Windows Phone including messages and the App Catalog
- MaaS360 User Identity Certificate distribution for email access, VPN access, or wifi access based on the configured MDM policy
- Distribution and installation of Enterprise Silverlight apps (.xap) that are compiled from the Windows Phone 8.1 SDK in the MaaS360 App Catalog
- MaaS360 Email for Windows Phone (Store app)
- MaaS360 Browser for Windows Phone (Store app)
- MaaS360 Docs for Windows Phone (Store app)

Services that remain unaffected

- Limited MDM capabilities that do not require the Symantec Mobile Code Signing Certificate are still available.
- No impact on the management of Windows desktops, laptops, or tablets.

Platform

EULA policy management >>

MaaS360 adds support in the WorkPlace Persona policy that allows administrators to upload an end user license agreement (EULA) usage policy as an HTML file. This policy also supports new settings such as usage policy expiration grace period (in days) and actions that are taken on devices if they do not accept the usage policy. You can also configure how often email reminders and prompts messages are displayed on the device about the usage policy when the user launches the app on their device.

Ability to delete administrator roles from the MaaS360 Portal >>

MaaS360 includes capability from the portal to delete a custom role that is associated with an administrator account. Previously, a role that is associated to an administrator account cannot be deleted and the role had to be unassigned from the administrator account to successfully delete the role.

Note: If an administrator account is associated with only one role and if the role is deleted, then the administrator account is made inactive. Contact IBM MaaS360 Customer Support Team to activate the administrator account again with Read-only role.

Custom range value expandable up to 90 days for data filters in patch management >>

MaaS360 expands the custom value range for the attribute "source release date" from 30 days to 90 days. Using this custom value, you can now filter patch management reports based on source release date from up to 90 days.

Cognitive recommendations for creating policies >>

MaaS360 suggests a cognitive policy based on your industry, deployment size, and area. You can enhance your existing policies with the community-derived policies. The policy recommendations indicate if your peers are following better approaches. If you are new to policies, you can easily start from a policy that is based on community-based recommendations to make sure that you are inline with industry standards.

Accessibility matrix for editing branding elements >>

The accessibility matrix allows Master Administrators and Partners to edit properties of the branding elements. The following levels of hierarchy are available for editing branding elements:

- Master Administrator (edit)
- Partner (edit)
- Customer (view)

Azure Active Directory integration >>

MaaS360 provides additional support for Azure Authentication and AD/LDAP Authentication mixed-mode setup.

Cloud Extender 2.99 Release Summary

No new features were introduced in this release. The following issues were fixed in this release:

-Fixed LDAP connection issues in Cloud Extender.

-Fixed issues with the IDnomic certificate integration.

-Fixed issues with intermittent failures when upgrading Mobile Enterprise Gateway (MEG) and Cloud Extender.

Cloud Extender 2.98 Release Summary

No new features were introduced in this release. The following issues were fixed in this release:

-Cleaned up duplicate mailboxes and devices resulting from the Get-CASMailbox change by Microsoft.

-Fixed an issue with the appearance of duplicate/additional Exchange ActiveSync records that blocked mail and the failure of the SecureMailEnabled web service.

-Fixed an issue with Auto Quarantine not working even though the setting was enabled in Cloud Extender.

-Fixed an issue where the Use Proxy Authentication setting displayed Yes in the MaaS360 Portal even though the proxy settings were not enabled in Cloud Extender.

-Fixed an issue where TLS 1.0 and TLS 1.1 were enabled in Mobile Enterprise Gateway (MEG).

Cloud Extender 2.97 Release Summary

New method for obtaining certificates from Microsoft Certificate Authority servers >>

The Certificate Integration module now provides an alternative to the SCEP method for requesting device certificates from a Microsoft Certificate Authority server. The Cloud Extender provides a feature that directly obtains certificates from Microsoft Certificate Authority servers that reside in the same forest, or trusted forests, as the Cloud Extender server.

iOS Release Summaries

2019 iOS Application releases for MaaS360

iOS Release Summaries

Release information for MaaS360 iOS Applications

iOS 3.97 Release Summary

MaaS360 makes the iOS app version 3.97 beta available to from iTunes on December 13, 2019.

MaaS360 for iOS (core app) Enhancements

Enhancements to shared mailbox delegate permissions >>

Prior to 3.95, when a delegate is added, the delegate has full access to all the folders by default. In 3.95, MaaS360 added folder-level permissions, allowing the users to set folder-level mailbox permissions for shared folder. However, MaaS360 did not support group-based folder permissions. As a result, the shared folders were unavailable to all the users in the group. In 3.97, MaaS360 adds a fix wherein administrators can use advanced security policies to allow the delegates to view only the Inbox folder.

Enhancements to report phishing emails feature >>

In 3.96, MaaS360 added support to allow users to report suspicious emails to administrators. In this release, MaaS360 adds support to allow administrators to configure report phishing settings directly through security policy settings instead of advanced policies. MaaS360 also allows administrators to configure if they want to receive the suspicious email as a forwarded mail or as an attachment.

Note: The advanced configuration setting **phishingReportingEmail** that was introduced in 3.96 is not supported anymore. Administrators must republish the persona policy with new settings.

Better error messaging for password lock and expiry usecases >>

As a part of our continued efforts to improve user experience, MaaS360 now provides better messaging for errors during the authentication process resulting from expiration of password or locked user account. Previously, a generic error message was displayed. Effective 3.97 release, the error messages ***Your password expired. Contact your IT administrator*** and ***Your account is locked. Contact your IT administrator*** are displayed for password expiration and locked user account respectively.

iOS Secure Browser 2.90 Release Summary

MaaS360 will make the Secure Browser app version 2.90 available beta is available on Test Flight on December 11, 2019.

Defect Fixes

37243	Fixed a Japanese translation issue for Home button.
36898	Fixed an issue where a blank screen was displayed when an intranet website that uses ***en*** (English) locale was opened.
36615	Fixed an issue where users could not login to an intranet site that used Mobile Enterprise Gateway (MEG) for authentication.
38074	Fixed an issue where Secure Browser did not load home page in Kiosk mode.

iOS 3.96.70 Release Summary

MaaS360 makes the iOS app version 3.96.70 available to from iTunes on December 9, 2019.

Beta will be available on December 4, 2019

Defect number	Description
37969	After upgrade of iOS 13, policy enforcement of **Restrict export of managed content and email attachments** fails.

iOS 3.96.62 Release Summary

MaaS360 makes the iOS app version 3.96.62 available to download/upgrade from iTunes on October 30, 2019.

Defect number	Description
37038	Fixed a mail sync issue for Office365 "US" (non outlook.office365.com server) domain accounts in Secure Mail.

iOS 3.96.52 Release Summary

MaaS360 makes the iOS app version 3.96.52 available to download/upgrade from iTunes on September 19, 2019.

Defect Fixes

Defect number	Description
37134	Fixed an issue wherein users were unable to sync MaaS360 email if they changed Mail password after upgrading to 3.96.40.

iOS 3.96 Release Summary

MaaS360 makes the iOS app version 3.96 beta available to download/upgrade from iTunes on August 12, 2019.

MaaS360 for iOS (core app) Enhancements

Certificate-based authentication support for share extension

MaaS360 now allows users to share files to Secure Mail via Share extension without prompting users to switch to MaaS360 app for authentication if Secure Mail uses certificate-based authentication. Previously, when a file was shared to MaaS360 Mail, an error message was displayed, and the file was saved to Outbox.

Note: In SMIME with cert setup, if the user has sent an email from the Compose screen to a recipient earlier, MaaS360 downloads that receiver's certificate and uses the certificate while sending a document via MaaS360 Mail Share extension. As a result, the documents do not end up in the Outbox.

Preview file when importing files into MaaS360 from third-party apps >>

When the files are imported into MaaS360 app from a 3rd party app, MaaS360 now allows users to preview the file and perform actions specific to the file type in the preview mode.

Report email as spam >>

MaaS360 now allows users to report suspicious emails to the administrators. The emails that are reported as spam are automatically sent to the administrators and then deleted from the Inbox. Administrators can use advanced settings in Persona policy to specify the email account that receives the report messages.

Permissions required to use location services in the background >>

With iOS 13, users need to explicitly grant permissions to allow apps to track location in the background.

iOS Browser 2.80 Release Summary

MaaS360 will make the Secure Browser app version 2.80 available on iTunes on August 23, 2019.

MaaS360 adds iOS 13 compatibility support and fixes minor defects.

Defect Fixes

35556	The PDF files in OneNote online are successfully opened in Secure Browser.
35489	The podcasts and videos are successfully played on Secure Browser in Fullscreen and inline modes on iPhones and iPads.
34556	The PDF files on intranet sites are successfully downloaded through Secure Browser. Previously, the Save to Docs option was unavailable on some intranet sites.

iOS 3.95 Release Summary

MaaS360 makes the iOS app version 3.95 available to download/upgrade from iTunes on June 28, 2019.

MaaS360 for iOS (core app) Enhancements

PIM delegate permissions >>

MaaS360 adds support for delegate permissions to allow managers to set permissions at folder level for delegates to read, delete, and edit items for Mail, Contact & Calendar.

Enhanced access to document export options with fewer clicks >>

MaaS360 enhances the usability by reducing the number of clicks required to access attachment and document export options across Secure Mail and Secure Docs apps.

Multi-language case-insensitive search support for Secure Mail >>

MaaS360 enhances email search by providing case-insensitive search support for Secure Mail. This feature allows users to perform a local search against To, From, Subject, and All fields in all languages supported by MaaS360. In the previous releases, MaaS360 only supported case-sensitive search for languages other than English.

Configuration of Office 365 endpoint URL >>

MaaS360 adds support for configuration of Office 365 endpoint URL through Secure Mail Configuration settings. Administrators can configure Office 365 endpoint URL to access the Office 365 API invocations for the Office 365 account.

Note: The default endpoint URL for Office 365 is https://outlook.office365.com. You must use a different endpoint URL than the default endpoint URL. On upgrade, an authentication prompt is displayed.

iOS 3.95.102 Release Summary

With MaaS360 for iOS 3.95.42, some users encountered an issue wherein after restarting the device, if the device received any actions while it is locked, the app entered selective wipe state.

Users must perform one of the following actions to fix the issue:

- Issue a selective wipe and revoke selective wipe action to the device.
- Delete the existing MaaS360 app and reinstall with MaaS360 for iOS app version 3.95.102.

iOS 3.80 Release Summary

MaaS360 for iOS 3.8 release summary
MaaS360 will make iOS app version 3.8 beta available in iTunes on November 30, 2018.

The MaaS360 for iOS app version 3.8 includes the following features:

MaaS360 for iOS (core app) Enhancements

MaaS360 app for Apple Watch >>

MaaS360 releases its first version of Apple Watch app, allowing the users to manage emails and calendar on the go. With this new app, users can seamlessly view emails, respond to emails, and view calendar events. Note: This feature is not enabled by default. Contact the MaaS360 support team to enable this feature for your account. After you enable the MaaS360 app on Apple Watch, the content is automatically synced from your iOS device to the Apple Watch.

Custom suggested shortcuts for MaaS360 app >>

MaaS360 identifies a set of custom shortcuts for commonly performed tasks in Docs, Secure Mail, Document, and Assistant apps that you can add to the Siri app. Note: The feature is supported only on iOS version 12 and above and applicable only for primary accounts.

Calendar

Support for Work week view >>

MaaS360 adds support for the Work week view - the days that are spent working in a week. A general work week starts from Monday through Friday. If an organization has a non-traditional schedule, MaaS360 allows users to set their own work days. With this feature, MaaS360 displays only the events and meetings for the working days.

Support to edit imported calendar events >>

In the previous releases, MaaS360 added support to sync events from the native calendar to allow users to view personal and work events in the MaaS360 Calendar. The events that were imported from the personal calendar were available for read-only. In this release, MaaS360 allows users to edit and delete the personal events directly in the MaaS360 app without having to switch to the native calendar app. **Note**: The changes are automatically updated in the native calendar app.

Support to change the meeting time to proposed time >>

In the previous releases, MaaS360 added support to allow the attendees to propose a different time if the meeting invite conflicts with another meeting on their calendar. In this release, MaaS360 allows the organizers to see all proposed times for all attendees and change the meeting time to one of the proposed times. **Note**: The feature is only supported on Exchange 2016+ and Office365 servers that use the new ActiveSync 16.1 protocol.

Secure Mail

Granular notification groups >>

MaaS360 adds on top of iOS per-app notification grouping feature to provide a more granular approach for email and calendar notifications. With this feature, MaaS360 smartly stacks the notifications in the Notification Center based on the predefined conditions: VIP and high priority emails, meeting messages, all other emails, calendar meeting reminders, and pending task reminders. **Note**: The feature is supported only on iOS version 12 and above.

Email quick responses >>

MaaS360 adds support for quick responses, allowing the users to respond to the emails with the predefined responses when they are busy. The users can select from the existing response or create their own responses.

Contacts

Support for Homepage field >>

MaaS360 adds support for the Homepage field of type URL, allowing the users to provide a web address for a contact.

Misc

32-bit architecture support deprecation >>

The MaaS360 iOS v3.8 app has deprecated 32-bit architecture.

iOS 3.85 Release Summary

MaaS360 makes the iOS app version 3.85 beta available to download/upgrade from iTunes on January 22, 2019.

The MaaS360 for iOS app version 3.85 includes the following applications:

- MaaS360 core app

MaaS360 for iOS (core app) Enhancements

Additional Usage (EULA) policy settings - iOS >>

MaaS360 adds support for usage (EULA) policies, allowing the administrators to grant conditional access to corporate shared devices upon consent to the usage policy. With this support, administrators can create new usage policies and enforcement actions that must be applied on the devices on non-acceptance of those policies. MaaS360 provides a complete view of license agreement status: Expired, Rejected, Accepted, Read only and Pending at the device level. You can also configure the frequency at which email reminders and prompt on app launch can be shown about the modified usage policy. For more information, see Persona policy settings.

MaaS360 iOS agent behavior on account termination

Until this release, if a MaaS360 portal became inactive, devices would still pass webservice calls updating information such as location data and compliance updates. With 3.85 the application will no longer share data via webservices with an inactive portal, and all communications between the MaaS360 portal and the iOS agent are blocked. Existing corporate data synced locally to the app will remain until the user manually deletes the agent.

Defect fixes

Defect	Summary
33971	The email accounts created with the %upn% placeholder via Persona policy are successfully configured on the device.
33831	MaaS360 delivers banner notifications to only those users that have permissions to a delegate account. Administrators can configure the advanced policy to completely disable the notifications for delegate account. Navigate to Security > Policies > Persona Policy > WorkPlace > Security > Configure Other Settings and provide the following key in the Advanced Configuration Details field. Key: iOSEnableDelegateEmailNotifications Value: No
33821	Users can successfully delete the emails while the device is placed in the Landscape mode. Previously, the Secure Mail app was terminated when the emails were deleted.
33611	The unread email counter is successfully updated in the Secure Mail app.
33083	The Exif data is retained when a photo is uploaded to email or Docs.

iOS 3.86 Release Summary

Defect fixes

Defect	Summary	Notes
34391	Users can successfully authenticate the MaaS360 app with TouchID. Previously, the authentication failed if the passcode contained a specific set of special characters (!#$%^&*).	After upgrade to 3.86 MaasApp PIN Screen would be presented once without Touchid. Going forward from second time Pin & Touchid prompt will be presented to the user.

iOS Browser 2.61.3 Release Summary

MaaS360 will make the Secure Browser app version 2.61.3 available on iTunes on 26 March 2019.

- This release includes minor security improvements.

iOS Browser 2.60 Release Summary

MaaS360 will make the Secure Browser app version 2.60 beta available on iTunes on 07 February 2019.

This release consists of the following features:

Account termination behavior on Secure Browser

After the MaaS360 account termination, MaaS360 stops the web-service calls made from the Secure Browser app to the MaaS360 portal. As a result, all the communications between the MaaS360 portal and Secure Browser are blocked. Also, MaaS360 blocks users from accessing any websites on the Secure Browser.

Time-based policy support for Secure Browser >>

MaaS360 extends the time-based policy support to Secure Browser. The time-based policy support allows enforcement of persona policies based on the time period. Administrators can restrict access to corporate resources via the Secure Browser app on the basis of the selected time of the day or days of a week. For example, administrators can deny access to corporate resources via the Secure Browser outside of the office hours.

32-bit architecture support deprecation >>

Effective 2.60 release, MaaS360 deprecates Secure Browser app on devices that support 32-bit architecture.

GDPR compliance privacy statement added in Browser settings >>

MaaS360 adds General Data Protection Regulation (GDPR) compliance privacy statement in the Secure Browser settings.

Certificate-based authentication support for iOS Secure Browser >>

MaaS360 adds support for cert-based authentication, allowing the users to automatically authenticate the websites using identity certificates. MaaS360 supports two types of certificates for authentication: Cloud Extender and PIV-D. Administrators can leverage Cloud Extender and Entrust portal/Purebred portal to push respective certificates to the devices through the MaaS360 portal.

Defect Fixes

Defect number	Summary
S-90459	Users can now successfully authenticate the Secure Browser app with Face ID.
33488	The Secure Browser app is successfully activated even if the password contains special characters.
33615	Users can now successfully authenticate and access sites that require Kerberos authentication. Users will be prompted to provide domain name in addition to username and password for authentication.

Known Issues

- With MaaS360 app for iOS 3.86, the Secure Browser app freezes at the activation screen if a passcode was not set on the devices through policies.

iOS 3.87 Release Summary

MaaS360 makes the iOS app version 3.87 beta available to download/upgrade from iTunes on March 11, 2019.

Defect fixes

Defect	Summary
34818, 34814, 34810	Fix for the issue where PIM (mail, calendar, contact) icons were not displaying in the agent with no PIN present.
34856	Fix for the browser issue where the app would get stuck at the activation screen if a passcode was not set on the devices.

iOS Secure Editor 2.60 Release Summary

MaaS360 will make the Secure Editor app version 2.60 beta available on TestFlight on 20 March, 2019.

This release consists of the following features:

Time-based policy support for Secure Editor >>

MaaS360 extends the time-based policy support to Secure Editor. The time-based policy support allows enforcement of persona policies based on the time period. Administrators can restrict access to corporate resources via the Secure Editor app on the basis of the selected time of the day or days of a week. For example, administrators can deny access to corporate resources via the Secure Editor outside of the office hours.

Render CSV files in Secure Editor >>

MaaS360 adds .csv to the list of file formats supported by Secure Editor. With this support, users can open and view the .csv file content through Secure Editor.

Secure Editor account termination behavior >>

When the account is terminated, the Secure Editor app will no longer share data via webservices with an inactive portal, and all communications between the MaaS360 portal and the Secure Editor are blocked. Existing corporate data synced locally to the app will remain until the user manually deletes the agent.

32-bit architecture support deprecation >>

Effective 2.60 release, MaaS360 deprecates Secure Editor app on devices that support 32-bit architecture.

Print documents from Secure Editor >>

MaaS360 now allows users to print all documents that are supported by Secure Editor except .txt files.

Defect Fixes

Defect number	Summary
31681	The flow charts are successfully rendered in Secure Editor.

iOS 3.90 Release Summary

MaaS360 makes the iOS app version 3.90 beta available to upgrade from TestFlight on March 22, 2019.

This release includes the following features:

Support to respect iOS device font resize setting in PIM >>

MaaS360 now respects the iOS device Large Text accessibility setting to adapt the corresponding text size across the PIM apps (Mail, Calendar, Contact, Tasks, and Notes). **Note**: The feature is only applicable to the English language and supported only on iOS 11 and later.

Defect Fixes

Defect number	Description
34813	The changes that are made in a document are now successfully synced between SharePoint and MaaS360.
34622	The email drafts are successfully synced between Outlook and Secure Mail.
34415, 34295	The photos on the device can be now shared through MaaS360 using the Share extension.
34301	The macro-enabled spreadsheet (.xlsm) files are accessed through the doc sources in Secure Docs.
33260	The Japanse characters are successfully rendered in .CSV files in the Secure Mail app.

iOS 3.91 Release Summary

MaaS360 makes the iOS app version 3.91 available to upgrade from TestFlight on May 14, 2019.

This release consists of the following defect fixes:

Defect number	Description
35106	Fixed an issue wherein the calendar invites were cancelled for new attendees when an existing attendee tentatively accepted a meeting update.

iOS Secure Browser 2.70 Release Summary

MaaS360 will make the Secure Browser app version 2.70 beta available on TestFlight on 31 May, 2019.

The release consists of the following defect fixes:

Ticket	Description
35808	Administrators can now whitelist the Wallet app and .pkpass file type to allow users to access boarding passes (.pkpass files) through the Wallet app even though data export is restricted. Previously, the whitelisted file types could not be accessed through the whitelisted third-party app when the data export was restricted.
35489, 27859	MaaS360 enables the Inline Playback setting in Secure Browser by default to play the videos and live stream hosting on iPhone and iPads. Previously, users had to turn on this setting manually. Behavior changes from previous release: The videos will now play inline by default on iPhones and will not automatically enter fullscreen mode when playback begins. However, users can tap the full screen icon to play the videos in the full screen mode.
35476	The email attachments are successfully opened when the emails are accessed through Secure Browser.
35124	The intranet sites are successfully opened when Mobile Enterprise Gateway (MEG) is enabled in Secure Browser.
35003	The Office attachments on Notes Web mail are successfully accessed through Secure Browser.
29568	MaaS360 now allows administrators to configure default timeout value in MEG, so that the intranet sites remain connected without terminating. To configure default timeout value (in seconds), Navigate to WorkPlace Persona policy > WorkPlace > Security > Advanced Configuration Details and provide the following details: **Key**: OverWriteTimeOutForGWTunneling **Value**: Desired value in seconds.
34952	MaaS360 now allows administrators to disable alerts on the intranet sites. Previously, an error message was displayed when intranet sites that are connected via MEG were accessed. To disable alerts, Navigate to WorkPlace Persona policy > WorkPlace > Security > Advanced Configuration Details and provide the following details: **Key**: shouldSkipAlertForErrorCodes **Value**: Yes/No

Android Release Summaries

2019 Android agent release summaries for MaaS360

Android 6.90 Release Summary

MaaS360 makes the Android app version 6.90 available in Play Store on 6 December 2019.

MaaS360 for Android core

Enterprise app management made easier with Managed Google Play iFrame (newer version) >>

MaaS360 enhances administrative experience for customers looking to publish applications to Android Enterprise devices using a newer version of Google's Managed Play Store iframe. In the new version, administrators can browse and publish apps in a simplified and secure manner by directly uploading them to Managed Google Play Store. With this feature, MaaS360 makes Managed Google Play the single source of applications for Android Enterprise deployments for all use cases- Device Owner (DO), Profile Owner (PO) and Corporate-Owned, Single-Use (COSU). The option to add public apps via the regular Google Play Store (retail), which was redundant, has also been removed for Android Enterprise customers. There will not be any impact to apps added using regular Google Play Store option.

In the previous releases, MaaS360 displayed options to publish public apps via Managed Google Play Store or regular Google Play Store. Effective 10.76, Android Enterprise customers will publish apps via Managed Google Play Store and non-Android Enterprise customers will continue to publish apps via regular Google Play Store.

Note: The change will impact only Android Enterprise customers. Some features in iframe 1.0 have been deprecated by Google such as ability to auto-accept new permissions for future app versions and receive email notifications when there are permission changes. As a result, administrators must accept the new permissions from App Catalog manually.

Publish private and web apps directly from Managed Google Play Store >>

MaaS360 has now extended support for publishing private apps and web apps using Managed Google Play iframe. The web apps are now distributed to the devices as regular native Android apps. With this support, administrators can publish private LOB (Line-Of-Business) apps directly from MaaS360 without having to switch to Google Play Developer console.

When a private app is published,

- Google creates a Play Console account on behalf of your enterprise and waives the $25 USD registration fee.
- The app is automatically approved for your organization.
- The app is ready for distribution in approximately 10 minutes.

Streamlined Device Administrator (DA) to Work Profile (PO) migration process

MaaS360 enhances the user experience of Android Enterprise migration tool by adding new screens during Device Admin to Work Profile migration process to make different stages of migration transparent to the user. The stages include re-registration of device, completion of Android Enterprise activation, migrating of logs, activation of Samsung Knox License, finishing setup and so on. This also makes it useful for users who would like to estimate the time taken for setup based on current state or get help for any troubleshooting purpose.

Note: In typical cases, each stage is displayed in a new screen that only lasts for few milliseconds and is hardly noticeable.

Re-authentication of Android Enterprise accounts on account expiration >>

In rare circumstances, Managed Google Play account could be invalidated on devices due to a number of reasons. In these cases, MaaS360 provides a provision for re-authentication of the work account. Specifically, in cases where the accounts expire, users are restricted from accessing Managed Play Store and new apps cannot be installed.

Better error messaging for password lock and expiry usecases

As a part of our continued efforts to improve user experience, MaaS360 now provides better messaging for errors during the authentication process resulting from expiration of password or locked user account. Previously, a generic error message was displayed. Effective MaaS360 for Android 6.90 release, the error messages ***Your password expired. Contact your IT administrator*** and ***Your account is locked. Contact your IT administrator*** are displayed for password expiration and locked user account respectively.

Enhancements to Kiosk notification badge count >>

In the previous releases, MaaS360 added notification badge support for third-party apps deployed in traditional kiosk mode or Android Enterprise COSU mode. This feature provided ability for users to subscribe to badge notifications such as missed calls or new email alerts for critical applications when using kiosk mode, especially when notification bar was disabled.

Adding to this feature, in the 10.76 release, MaaS360 extends notification badge support to all first party apps including MaaS360 Email and Messages.

In order to support unmanned usecases, where devices may not have a user to turn on such notifications, MaaS360 also adds a new Kiosk/COSU policy **Show App Badges** to allow the administrators to restrict the display of Show/Hide app badges option in kiosk settings on the device. This policy is turned ON by default. When the policy is OFF, the **Show App Badges** option in Kiosk/COSU settings is unavailable to the end-users.

Lock screen management policies support for devices enrolled in Profile Owner (PO) mode >>

MaaS360 extends keyguard management policies to Profile Owner (Work Profile) devices. In the previous releases, these policies were only applied to Device Owner (DO) devices.

Note: Supported on Android 9 and later devices.

Azure multi-factor authentication (MFA) support to enroll users into MaaS360 >>

In previous releases, MaaS360 only supported a single type of enrollment workflow where MaaS360 automatically authenticated a user by using the user's username and password credentials or SAML to enroll users into the MaaS360 Portal. Effective 10.76, MaaS360 also supports Azure multi-factor authentication for the enrollment workflow, where authentication is delegated to Azure. As a part of this, the user is re-directed to an external Microsoft Login page to enter their username/password credentials, authenticated by Azure, and then redirected back to MaaS360 to continue with enrollment.

Note: This feature is not available by default. To enable this feature, contact your IBM MaaS360 Account Manager or IBM MaaS360 Support. Both types of enrollment workflows are not supported on the same customer tenant. If the feature is not enabled for your account, you will continue to enroll devices through your existing enrollment workflow using the MaaS360 enrollment page.

New policy to allow or disable the use of Airplane mode on Bluebird devices >>

MaaS360 extends the **Allow Airplane Mode** policy to Bluebird devices that are enrolled in Device Administrator mode. This policy allows administrators to remotely enable or disable the use of Airplane mode on devices.

Path: Android MDM policy > Device Settings > Restrictions >Network Settings > Allow Airplane Mode.

Note: Requires MaaS360 for Bluebird app version 6.90.

Announcement: Expect changes around Device Enrollment Mode in Device Summary for Android Enterprise devices

Until now, within IBM MaaS360 portal, for Android Enterprise use cases, both the attributes **Enrollment Mode** and **Container Type** on Device Summary page were showing up as **Device Owner** and **Profile Owner** for DO and PO deployments respectively. These values clearly represent the type of container deployed on these devices and do not pertain to mode of enrollment.

Going forward, **Enrollment mode** attribute will start reporting actual enrollment mode for devices where the mode is available/known to MaaS360 app. Hence, **Container type** attribute shall be used in Device Summary page and in Advanced Search workflow to filter Device Owner and Profile Owner devices using *Hardware Inventory* > *Container Type* selection.

In **Devices** > **Groups** workflow, or within the custom watch list in the home page, customers who are currently using **Device Enrollment Mode** to track and group Device Owner and Profile Owner devices are requested to move to use **Container Type** attribute to filter container type on the device in order to ensure that any policy/rule assignments and application/document distributions remain intact.

In order to start tracking accurate device enrollment modes, going forward re-generate QR code and Zero Touch JSON profiles at least once and use MaaS360 for Android 6.90+.

In the next release, i.e., 10.77 Portal release, MaaS360 will be rolling out the change to read the right value for **Enrollment Mode** as **QR Code**, **Google Zero Touch**, **Knox Mobile Enrollment**, **NFC** or **DPC Identifier** (for AFW#) where information is available at the client side.

Impact after 10.77 Portal release

- Customers using **Device Enrollment Mode** attribute in device groups or home page watch lists are requested to change the attribute filter criteria to **Container Type** instead of **Device Enrollment Mode**.
- For devices running MaaS360 for Android versions below 6.90, and where administrators have not re-generated QR code or ZT JSON profiles, the enrollment mode isn't available already, so the device summary and smart search will show " **Device Enrollment Mode**" attribute value as **Not Available**.
- We are also fixing the behaviour on legacy Device admin enrollments, where Enrollment Mode was always **Manual**. You will start to see **Android Configurator** where applicable. We will be introducing **Container Type** attribute for Device Admin devices which will read any one among following values - **Device Administrator**, **Samsung Device Administrator**, **Honeywell Device Administrator**, **Bluebird Device Administrator**, etc, where OEM SDK is integrated.

Android 6.82 Release Summary

MaaS360 makes the Android app version 6.82 available in Play Store on 12 November 2019.

- Zero-day support for Samsung Android 10 OS
- Bug fixes and security fixes

Android 6.80 Release Summary

MaaS360 makes the Android app version 6.80 available in Play Store on 3 October 2019.

MaaS360 for Android core

Kiosk launcher gets redesigned settings (gear) icon and notification badge support >>

MaaS360 displays notification badges for Kiosk apps, informing users that outstanding notifications are available for the apps. This will inform users if they have missed calls or unread emails in the absence of other kind of notifications when such apps are assigned in kiosk mode.

The Kiosk launcher gets a redesigned Settings (gear) icon that stands out on any background.

Disabled capturing of enrollment screens to protect sensitive data

When the app enters background during the enrollment, the confidential data on the enrollment screen is hidden until the user resumes the screen. Users are also prevented from capturing the screenshots of enrollment screens.

Unlock WorkPlace with Iris and Facial recognition >>

MaaS360 supports new forms of biometric authentication such as Iris and Facial recognition in addition to fingerprint scan for WorkPlace authentication on Samsung devices.

MaaS360 app exempted from battery optimization on Samsung SAFE 5.7+ devices

MaaS360 core app is by default exempted from battery optimization. The app does not enter the battery saving mode even though the app is not accessed for longer periods.

MaaS360 app now supports direct boot mode

Administrators can now issue commands such as device wipe, reset passcode, and profile wipe while the device is in direct boot mode. **Note**: Supported only on Android devices running OS version 7+ and enrolled in Android Enterprise (DO or PO) modes. Samsung devices support device wipe action and do not support reset passcode action. It takes around 4 to 5 hours for the action to reach the device in direct boot mode.

Reset passcode changes for Samsung Knox 3.2.1+ devices enrolled in Device admin mode >>

MaaS360 uses new API provided by Samsung to reset password on Samsung Knox 3.2.1+ devices that are enrolled in Device Admin mode.

Unlock WorkPlace with Iris and Facial recognition >>

MaaS360 supports new forms of biometric authentication such as Iris and Facial recognition in addition to fingerprint scan for WorkPlace authentication on Samsung devices.

App Management

Deep links support for installation of apps on Android agent >>

With MaaS360 for Android 6.80+, administrators can create deep links that allow installation of Google Play and Private apps on Android Enterprise (DO or PO) devices. With this support, users can bypass the app catalog and initiate the app installation by just tapping the deep link sent by the administrator. **Note**: The app that is being installed must be available in the end-user app catalog. The deep link must have all necessary parameters. The device must be enrolled either in DO or PO modes.

Android 6.70 release summary

MaaS360 makes the Android app version 6.70 beta available in Play Store on 2 July 2019.

MaaS360 for Android core

Android Enterprise Migration Program: General Availability of DA to Work Profile migration >>

MaaS360 announces the general availability of Device Admin (DA) to Work Profile (Android Enterprise Profile Owner) migration. In the second phase of series of enhancements, MaaS360 adds support for migration of multiple devices at once (group action), enforcement of Work Profile migration (force migration after 90 days), activation of Samsung Knox License (SKL) as well as track granular migration status in the Action history as a part of migration. Note: Requires MaaS360 for Android agent version 6.70 and later.

Android Enterprise as the default enrollment mode >>

MaaS360 now allows administrators to make Android Enterprise the default enrollment mode for the organizations that want to move off the Device Admin deployment mode and adopt Android Enterprise. MaaS360 also displays an alert message in the home page if Android Enterprise is not setup. For new customers, Android Enterprise must be set up in the MaaS360 portal to complete Android Enterprise enrollments on the device. The existing customers can contact MaaS360 Account Representative to enable this feature for their account.

Configuration of minimum operating system restriction for Android Enterprise self enrollments >>

MaaS360 adds support to allow administrators to drive the Android Enterprise enrollments based on the minimum OS version. This feature is helpful for the organizations that are implementing a phased adoption to Android Enterprise, wherein the latest OS versions can be pushed to Android Enterprise and the old versions can stay back on Device Admin deployment. Administrators can use the self enrollment options in the Device Enrollment Settings to configure the OS versions that are allowed to use Android Enterprise. When the end-users initiate the enrollment, the devices that meet the minimum OS requirement enroll into Android Enterprise (Work Profile) and the devices that do not meet the minimum OS requirement fall back to Device Admin deployment.

Support to block automatic system updates on Android Devices >>

MaaS360 adds support to block automatic system updates over a scheduled time to allow administrators to evaluate the new update for compatibility and bugs before rolling out to employees. Administrators can suspend system updates for up to 90 days. When a device is within a freeze period, the notifications about pending system updates are not received, the system updates to the OS are not installed, and the users are prevented from manually checking for system updates.

MaaS360 for Android includes various behavior changes as a part of compilation against Android OS version 10.

Location services auto-enabled in Android Enterprise enrollments >>

When a device is enrolled in Android Enterprise (DO and PO), MaaS360 automatically gains access to device location when the app is running in foreground and background. In Device Admin enrollments, users must explicitly grant location permissions to MaaS360. **Note**: Supported on Android Q and later devices.

Shared Device support for G Suite

The shared device feature is only supported on Android 9 Pie and later devices that are enrolled into Android Enterprise through G Suite account in corporate shared mode. The Sign In and Sign Out options are unavailable on Android devices running OS version below 9 Pie.

Validation of Google user account on the devices as a part of policy evaluation

MaaS360 now validates the status of managed Google account as a part of policy evaluation on the devices that are enrolled in both PO and DO modes . If the managed Google account is removed by the users, MaaS360 automatically creates the Google account for non-G Suite accounts and marks the device Out of Compliance (OOC) for G Suite customers, allowing the users to manually create the corresponding Google account.

Deprecation of devices that only use armeabi architecture >>

MaaS360 announces the deprecation of devices that only use armeabi architecture.

Secure Mail

Support to launch native dial pad on tapping the phone numbers >>

MaaS360 adds a new setting to allow users to directly launch the native dial pad on tapping the phone numbers across Secure Mail and Calendar apps. Previously, users had to manually choose the native dial pad from the app chooser dialog.

Android 6.60 Release Summary

MaaS360 makes the Android app version 6.60 beta available in Play Store on 4 April 2019.

MaaS360 for Android app version 6.60 includes the following applications:

- MaaS360 for Android core
- Secure Mail

MaaS360 for Android core

Support to approve or deny all app-level run time permissions in Android Enterprise >>

When the default runtime permissions are granted at the device level, Android only grants top-most permissions to the apps on the device. MaaS360 adds support to allow the administrators to approve or deny all run time permissions at an individual app level.

Support to assign a custom device name to enrolled Android devices >>

MaaS360 adds support for a new device-level action **Set Device Name**, allowing the administrators to change the name of the enrolled Android devices. Administrators can assign a custom device name that makes it easier for them to identify the devices at a glance.

Note: Supported on Android devices enrolled in both MDM and Android Enterprise.

Support to set default locale and timezone through QR code and Zero-touch enrollments >>

MaaS360 adds usability enhancements to the QR code and Zero-touch enrollment workflows, allowing the administrators to set a default locale and timezone during the enrollment. However, it must be noted that the users can change the locale and timezone on the device after the enrollment.

Support to restrict app installs to Google Play >>

MaaS360 adds a device-wide restriction to block the app installations through sources other than Google Play. When the **Allow device wide restriction on installation of apps from Non-Google Play** policy is applied, the app installations from unknown sources are blocked in both Personal Profile and Work Profiles. Previously, it was not possible for administrators to disallow the installation of apps from unknown sources in the Persona profile.

Note: This policy is only applicable to Android 9.0 and later devices enrolled in PO mode. The system settings remain active on the device, but the system blocks app installation. This policy only affects future installations so the apps that are already installed through unknown sources remain on the device.

Single sign on to G-Suite during Android Enterprise enrollment >>

MaaS360 adds cert-based authentication support for enrolling devices into Android Enterprise (G-Suite/Managed Google Account). G Suite customers leveraging IBM Cloud Identity can seamlessly authenticate the MaaS360 app during the Android Enterprise enrollment process. In the previous releases, when IBM Cloud Identity was used as the identity provider for G-Suite, the users had to authenticate the MaaS360 app with their Cloud Directory credentials.

Note: The user certificate is removed from the device after enrollment. Requires MaaS360 for Android 6.60 agent.

Support to control the maximum device enrollments allowed per user account

Recently, Google imposed a restriction on user accounts enrollment that it will support only a maximum of 10 devices per Android Enterprise user account. In accordance with this restriction, MaaS360 will show a warning message to the end-users when more than 10 devices are enrolled with the same user account. There may be a chance that end users may ignore this warning message and proceed with the enrollment.

In case you want to enforce the restriction in your organization, contact MaaS360 Support who can set this configuration to **Do not allow enrollment** when more than 10 devices are enrolled with the same Android Enterprise user account.

Real-time update of Android Enterprise approved apps

MaaS360 takes advantage of Google EMM Notification APIs to receive application updates notification for approved apps in near real-time. In the previous releases, MaaS360 relied on a batch job that was executed every 4 hours in a day and processed application updates (approved/unapproved) in 7 days interval.
Note: The apps that are not updated through Google EMM Notification APIs will continue to be updated through the batch job.

Secure Mail

Support to exclude MaaS360 Mail from battery optimization >>

MaaS360 allows users to turn off battery optimization for Secure Mail app. Previously, the battery optimization was turned on for Secure Mail by default. When the option is turned on, the device could not synchronize with the mail server constantly, resulting in delays in the email and notifications.

Android 6.50 Release Summary

MaaS360 for Android 6.50 Release Summary

BETA FEEDBACK :

Please fill out a feedback survey once BETA testing is complete (survey opens Jan. 22nd): https://www.securitylearningacademy.com/mod/feedback/view.php?id=14680

MaaS360 makes the Android app version 6.50 beta available in Play Store on 21 January 2018.

MaaS360 for Android app version 6.50 includes the following applications:

- MaaS360 for Android core
- PIM
- App Wrapping
- OEM

MaaS360 for Android core

Device Admin to Profile Owner Migration - beta >>

MaaS360 adds support to allow users to easily migrate from Device Admin to Profile Owner (PO) mode. It is recommended to adopt Android Enterprise and plan the migration in advance as Google announced the deprecation of Device admin for enterprise use starting in the Android 9 Pie release.

Migration from GCM (Google Cloud Messaging) to FCM (Firebase Cloud Messaging) >>

Google has announced decommissioning of GCM on April 11th, 2019. EMM vendors are mandated to move to Firebase Cloud Messaging (FCM) for providing real-time notifications to devices. As per Google mandate, MaaS360 will move to Firebase Cloud Messaging(FCM), which inherits the reliable and scalable GCM infrastructure, plus many new features. Firebase Cloud Messaging (FCM) is a new push notification mechanism for communicating with any Android app from a web server such as EMM.

Track-only mode for Trusteer Threat Management >>

MaaS360 adds a new remediation action to allow the administrators to only track the malware apps. The "Track only" action mode allows the administrators to keep a track of all devices running malware apps but not apply an automatic remediation action immediately. It neither creates a notification for the end user about malware detection nor puts the device in OOC state. The existing **Report** option has been renamed to **Report and OOC** to make the options clear and easy to understand. Previously, based on the policy setting, either the app was uninstalled or the device would go out of compliance automatically.

Support for tracking the Kiosk mode status >>

There have been multiple scenarios where administrators want to understand if kiosk mode is enforced on the device and also identify the current status of kiosk mode on the device. MaaS360 allows the administrators to easily track the stages of Kiosk mode through Kiosk Mode field in the Device View and also create advanced search criteria to filter the devices in Kiosk mode by the status.

EULA policy management >>

MaaS360 adds support for license management (EULA), allowing the administrators to grant conditional access to corporate shared devices upon consent to the usage policy. With this support, administrators can create new usage policies and enforcement actions that must be applied on the devices on non-acceptance of those policies. MaaS360 also provides a complete view of license agreement status: Expired, Rejected, Accepted, Read only and Pending at the device level. You can also configure the frequency at which email reminders and prompt on app launch can be shown about the modified usage

policy.

App Wrapping

App Wrapping: Support for apps compiled with AAPT2

MaaS360 now allows users to wrap the apps that are compiled with AAPT2 (Android Asset Packaging Tool), a build tool that Android Studio and Android Gradle Plugin use to compile and package the app's resources.

OEM

Support for Browser and Lockscreen Android Enterprise policies for Samsung KNOX devices

MaaS360 adds support for Browser and Lockscreen policies for Samsung Knox devices. These policies are distinguished with a new support tag PO with KNOX and DO with Knox under Android Enterprise Settings in Android MDM Policy.

SKL and KLM license management - beta >>

MaaS360 adds support for Samsung Knox License (SKL) license management, allowing the administrators to deploy the SKL license key to the Samsung devices. SKL is a consolidated license that is designed by Samsung to replace Enterprise License Management (ELM) and Knox License Management (KLM) licenses. Requires MaaS360 for Android 6.50 +, Knox 3.0 +.

Note: The feature is not available by default. Contact MaaS360 support team to enable this feature for your account. SKL key expiry is not handled yet by MaaS360. If you provide a key that is bound to expire soon, the users will be locked out of Profile Owner mode and encounter issues in the Device Owner mode. When the feature is enabled, all Android Enterprise enrollments on Knox 3.0 + devices require a SKL license and if the SKL key is not functional, the enrollments will fail.

PIM

Support to search emails with non-English characters

MaaS360 allows the use of non-English characters to search emails with the advanced search fields: **From**, **To**, **Subject**, **All without body**.

Note: Supported for primary, secondary, and delegate accounts. When the **To** field is used, MaaS360 searches against **To**, **CC**, and **BCC** fields. When the **From** and **To** options are used, MaaS360 searches against email sender names as well as email addresses.

Android 6.51 Release Summary

MaaS360 makes the Android app version 6.51 beta available in Play Store on 20 March 2019.

This release consists of the following defect fixes:

Defect Fixes

Defect Number	Description
35014	Fixed an issue wherein a black bar was displayed in the Secure Mail app while composing an email if the rich text editor was turned on.