10.80 Release Summary

iOS

Apple Shared iPad for business >>

With iOS 9.3, Apple introduced Shared iPad for education, allowing the students and teachers to sign into Shared iPads with their Managed Apple IDs that are created through Apple School Manager (ASM). With iOS 13.4, Apple extends the Shared iPad support to enterprises. With this support, administrators can use MaaS360 to securely deploy supported iPads in Shared mode. With Shared iPads, multiple shift workers in an organization to sign in/out of a single iPad with their unique Managed Apple IDs that are created through Apple Business Manager (ABM).

MAC address randomization >>

iOS 14 devices will now present a randomized Media Access Control (MAC) address for each Wi-Fi network (SSID). Administrators can use the **Disable MAC address randomization** setting in the Wi-Fi policies to disable the randomization of MAC address and send the actual MAC address while associating with the network. If true, a privacy warning is shown in Settings, indicating that the network has reduced privacy protections. If set to false, a random MAC address is sent to protect the privacy of the device and the user.

Android

Work profile on corporate-owned devices (WPCO) >>

Work Profile is a secure container that separates work apps and data from personal apps and data while maintaining user privacy. In the previous releases, Work Profile could only be set up on personal (BYOD) devices that are also used for work. With Android 11, the Work Profile capabilities - privacy protections, securing and separating work data are extended from employee-owned devices to corporate-owned devices. With this support, employees can securely use company-owned devices for personal activities without sacrificing privacy. Administrators have more device-level control in WPCO scenario as compared to that offered for Work Profile on Personally-Owned devices. For example, administrators can wipe the entire device and disallow app installations from unknown sources on the personal profile of the device.

Note: This feature requires MaaS360 for Android app 7.30+.

Changes to Device Enrollment Settings >>

With the previous design, the mixed-mode customers had to choose either Android Enterprise or activation as the default new device addition mode in **Device Enrollment Settings** for self-enrollments. In this release, MaaS360 revamped the **Device Enrollment Settings** to facilitate both activation and Android Enterprise enrollment for self-enrollment. For example, administrators can now have the corporate devices go through activation and employee-owned devices enroll in to Android Enterprise mode. In an effort to make the self-enrollment configuration experience easier, MaaS360 moved Android Enterprise self enrollment options from **Basic** to **Advanced** tab in the **Device Enrollment Settings**.

New group and device-level actions for Bluebird and Zebra devices enrolled in DO mode >>

MaaS360 now extends the Bluebird and Zebra group and device-level actions to Device Owner (DO) mode. With this support, administrators can remotely issue real-time actions such as push profile and push custom XML, and group-level actions such as copy file and push OS upgrade. In the previous releases, these actions were supported only on Device Admin devices. **Note**: Requires MaaS360 for Android app 7.30+.

COPE end-of-life

MaaS360 marks COPE mode for end-of-life with MaaS360 for Android 7.20. As a result, MaaS360 does not support new COPE (Corporate-Owned, Personally Enabled) enrolments, and the configuration options to enroll a device in the COPE mode are removed from the MaaS360 portal. Administrators will have to regenerate any old configuration profiles QR codes/JSON files which have the COPE flag set to true.

A step forward towards Device Admin deprecation >>

Google announced the deprecation of the legacy Device Admin for enterprise use effective with the Android 10 Q release. In an attempt to promote the adoption of Android Enterprise, MaaS360 makes Android Enterprise integration a prerequisite for all Device Admin enrollments for new customers. MaaS360 also displays banners at various places in the MaaS360 portal and blocks all Device Admin enrollments for end-users until the Android Enterprise is configured.

New group-level action to reboot devices >>

MaaS360 adds a new group-level action to allow administrators to remotely restart multiple devices at once. Supported only on Android (DO) devices. **Note**: The users are not notified of the restart in advance, so any work the users are on will be lost.

Disabled location tracking on PO devices >>

In the previous releases, the location permission was auto-granted to the MaaS360 app when Android 11 devices were enrolled in Profile Owner (PO) mode, and end-users could not revoke the location permission from MaaS360 Settings. Effective 10.80, MaaS360 does not auto-grant location permission during the enrollment and ensures that the permission is only granted when geofencing is enabled. **Impact**: When the location permission is not granted, the MaaS360 app cannot report the last connected SSID to the MaaS360 portal. **Note**: Requires MaaS360 for Android app 7.30+.

Support for new Android Enterprise keyguard policies >>

MaaS360 adds new Android Enterprise policies to remotely control the Keyguard features: Face recognition and IRIS recognition. **Note**: Supported on Android 9.0+ (PO and DO) devices. **Note**: Requires MaaS360 for Android app 7.30+.

Cross profile communication between apps >>

By default, MaaS360 does not allow communication between apps across profiles. For example, the Google Chrome app in the Personal profile cannot communicate with its instance in the Work Profile. MaaS360 now allows administrators to use the security policy **Allow cross-profile apps** to configure apps that support cross-profile communication. **Note**: Supported only on Android 11+ devices that are enrolled in PO mode. **Note**: Requires MaaS360 for Android app 7.30+.

Package delegation support for Android Enterprise apps >>

As a Profile Owner or Device Owner, the MaaS360 for Android app can now grant certain delegations to other apps. Delegated apps are apps that receive additional permissions such as installing existing packages, enabling system apps, etc, from the profile owner or device owner apps. **Note**: Requires MaaS360 for Android app 7.30+.

Display work events in personal calendar >>

With cross-profile calendar support, administrators can use the security policy **Allow work events on personal calendar** to allow the personal calendar to show events from the selected work profile apps. **Note**: Supported on Android 10+ devices enrolled in PO mode. **Note**: Requires MaaS360 for Android app 7.30+.

Support to collect preboot security logs for DO and WPCO devices >>

MaaS360 adds a new Android Enterprise policy **Enable Enterprise Security Logging** to allow administrators to track preboot security logs from Device Owner (DO) and Work Profile on Corporate Owned (WPCO) devices. **Note**: Requires MaaS360 for Android app 7.30+.

Added Samsung system apps to list of apps that are allowed by default on enrolled devices >>

MaaS360 now adds a set of Samsung system apps that administrators can configure to be included by default on enrolled PO and DO devices. To select Samsung apps, navigate to Android policy > **Android Enterprise Settings** > **App Complaince** > **Configure allowed system apps**. In the previous releases, Samsung apps had to be manually added as additional apps in the MaaS360 portal.

Enhancements to Factory Reset Protection (FRP) policy >>

FRP is a security feature that prevents unauthorized access to the device after a factory reset by locking the device to the Google Play ID that is configured in the device Settings. In the previous releases, the FRP policy was enabled by default without the knowledge of the administrators. When the policy was published without configuring the authorized accounts to override FRP, there is no way to unlock FRP on a DO enrolled device that has been factory reset. In this release, MaaS360 leaves the Factory Reset Protection policy unchecked by default for new customers.

Platform

Enhancements to the self-enrollment default ownership settings >>

In the **Basic Device Enrollment Settings**, an option to define the default ownership during self-enrollments is updated with the following options: **Employee owned**, **Corporate owned**, and **Prompt user for ownership**. Based on the default value that is selected here, the device ownership is considered for self-enrollment methods. Previously, only prompt user for ownership option was available and if this option was unselected, the device ownership was considered as corporate owned by default. With the enhancements made in this release, default device ownership can be set to employee, corporate owned or even allow user to define the device ownership during self-enrollment. Note: In case where 'By Ownership' is selected in 'Default new Device Addition Mode for Self Enrollment' mode, 'Prompt user for ownership' is applied as the default ownership mode and this setting cannot be changed.

End user portal shows Platform serial number and OS version device detail in the Device view >>

In addition to the existing device details in the Device View section of the End user portal (EUP), additional device details such as Platform Serial Number and Operating System Version are displayed. In cases where end-users have more than one device with the same device name, the platform serial number helps the user to uniquely identify the device. Additionally, the OS version shows the current version of the operating system on the device.

Device detail view summary >>

To aid Administrators the ease for viewing and accessing Device Summary details in the MaaS360 portal, the following enhancements are made;

- The drop-down in the Device View Summary is split across two columns for ease of viewing and accessing these device detail options in the Summary page.
- The device details drop-down in the Device Summary page is shown on the screen even on moving the cursor away. This drop-down does not disappear like before on losing the cursor focus. This accessibility enhancement is focused in aiding administrators to easily click the device summary option to view in detail.
- In the Device Inventory, a horizontal scroll bar is added in the Device View grid when the number of columns in the grid exceeds the grid table size. Previously, with more number of columns, the grid would auto-compress to fit the grid table size by which the readability of the device view details was compromised. With the horizontal scrolling in the Device View grid, Administrators can now customize to view any number of columns in the grid and also easily scroll to view all device details. **Note**: This horizontal scroll bar is shown in screen only when the number of columns in the grid exceed the grid table size.

Note: These enhancements do not include any functional changes to the device detail summary.

Customize session inactivity timer for an administrator logged-in session >>

To support Administrators to continue working on the MaaS360 portal without having to log in over and again due to session inactivity, MaaS360 adds **the Logout administrator sessions** option in the Advanced Administrator Settings. Use this setting to customize the allowed administrator session inactivity time. Currently, the maximum duration of session inactivity that is allowed is 2 hours, the minimum session inactivity that is allowed is 15 minutes, and the default minimum session inactivity of 30 minutes is allowed. When this session inactivity time is customized, a 2-minute timer is displayed during a logged-in inactivity session. This timer is shown 2 minutes ahead of the allowed session inactivity duration along with an option for an Administrator to either logout or to extend the current session. The allowed maximum session inactivity timeline will be increased in the future releases.

Enhancements around iOS User Enrollment feature >>

MaaS360 now makes it easy for the administrators to link Managed Apple IDs to the corresponding user records in bulk and send multiple User Enrollment requests at once. MaaS360 also adds minor enhancements to Enrollments and User Directory list view pages.

MaaS360 portal user interface theme is changed to cool grey >>

As per the latest survey for better user experience and improved viewability for Administrators to use MaaS360 portal, the portal theme is changed to cool grey. The grey theme change applies to the color in checkboxes, grids, calendar flyout, and so on, in the portal. This enhancement impacts only the color theme that is presented in the UI elements on the MaaS360 Portal. There are no functional changes to the workflows with the portal theme enhancement.

MaaS360 M1 and M3 Platform to utilize Akamai Kona Technology >>

With the 10.80 Release the MaaS360 M1 and M3 Platform will begin to utilize Akamai's Kona Technology, which is an industry-leading web application firewall (WAF) and distributed denial-of-service (DDoS) protection solution. Akamai's Kona Technology guards MaaS360 applications against the largest and most sophisticated attacks. It delivers proprietary rule sets and detection logic honed from Akamai's experience and investment in defending against the latest cyberattacks.

- ○
  - MaaS360 M1 Akamai Kona Technology Details
  - MaaS360 M3 Akamai Kona Technology Details

MaaS360 Product Suite will deprecate support for TLS v1.1 >>

The IBM MaaS360 Product Suites will be deprecating support for TLS v1.1 on December 4, 2020.

Analytics

Enhanced UI dashboards for Network reports and Hardware Inventory reports >>

MaaS360 offers improved UI experience for Network and Hardware Inventory reports and are available to all customers now. The functions of these reports remain the same as in old UI with enhanced UI design elements to offer better user experience with reporting capabilities. In addition to the enhanced UI, following capabilities are also offered;

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

Near-real time reporting for UEM Overview reports >>

MaaS360 extends real time reporting capabilities for UEM Overview reports. With this capability, the UEM reports are almost near real-time. Any updates in the statistical overview about devices across platforms are almost instantaneously reflected in these mobile device report dashboards.

App Management

Migration of auto-update configuration to the new design and its implication on administrators and end-users >>

The Auto-Update settings in the App Settings are redesigned to simplify the options and clearly demarcate the administrator controlled and end user controlled scope of app updates. The current configuration of customer's app settings has been migrated over to their preferred usage mode in the new revamped behavior. For more information on the new auto-update settings, see https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/pag_source/tasks/pag_apps_app_settings.htm

Old auto-update setting	New auto-update setting	Impact
User-Controlled Default Disabled	**Admin controlled**	**Impact on Users:** End users who had opted in for updates and used to get app updates for an app that was not marked for auto update by the administrator for ios enterprise apps and app store app would not get auto updates on the next upgrade of the app. End-users will no longer have an option of controlling updates. **Impact on Administrators:** The setting is now Admin Controlled which means asdministrators will have an app level control for auto update. Since auto update flag was not marked for ios public apps as true (as this option was not available to admins so far), in case the admin wishes to push out updates for existing apps, this setting can be edited. **Next steps:** Admin can review iOS public apps which needs to be auto updated on device & select "Update Automatically" flag in app summary.
User-Controlled Default Enabled	**User controlled**	**Impact on Users :** End users who had opted out of updates and used to get app updates for an app that was marked for auto update by the administrator for ios enterprise apps would not get auto-updates on the next upgrade of the app. End users continue to have an option of controlling updates. **Impact on Admin:** The setting is now User Controlled which means administrators will not have option to set "Update Automatically" for apps **Next steps:** No Action required

Windows

Scheduling the installation of Windows apps (MSI, EXE, BAT, downloadable files) from the App Catalog >>

MaaS360 enhances the *App distribution* workflow by allowing administrators to schedule the installation of apps on end user devices from the App Catalog. After apps are distributed to the App Catalog, administrators can choose which apps to install on end user devices, and specify whether to install those apps instantly on the device or schedule the app installation to start on a specific date and time of day over a staggered period of time to reduce the load on the network.

In the MaaS360 Portal, administrators can view the details for scheduling the app installation from the App Catalog by clicking More under the app, and then selecting Manage Distributions. Adminstrators can also view the installation status of an app on a device by selecting the device and then selecting Summary > App Distributions.

Note: The scheduling option only supports the installation of the following Windows distributed apps on Windows 10 MDM devices: EXE, MSI, BAT, and downloadable files (DOCX, PPTX, JPEG, PNG, XML, INIT). Windows Universal App Packages (APPX and APPXBUNDLE) and Windows devices that are managed by DTM are not supported.

App installation scheduling options:

Administrators can now set the following options to schedule the installation of distributed Windows apps from the App Catalog to a Windows device or a group of devices. When the scheduled date and time is set, the app is installed on the device.

- Start date: Select the date to schedule the installation of the distributed app on a Windows device or group of devices.
- Start time (0 - 23 hours): Select the local time on the device to schedule the installation of the distributed app to the device or a group of devices. The values include:
  - Immediately

- 00 (midnight or 12:00 AM) to 23 (11:00 PM)
- Distribute over (0 - 24 hours): Forces MaaS360 to space out the installation of distributed app binaries to devices over the selected hours to reduce the load on the network. The values include:
  - Immediately
  - 1 to 24 hours

Distributing Windows OS patches to groups of Windows devices >>

MaaS360 further enhances the *Patch management* workflow by providing an option that allows administrators to distribute patches to devices in a specific group that are missing the respective OS patch. Administrators continue to use the distribution and restart settings that were introduced in previous releases to distribute patches to device groups.

Note:

- If a new device is added to a group after a missing patch was distributed to that group, that device automatically receives the patch distribution.
- If a default device group has no group-level action taken on that group, then the group will not be displayed to the administrator as active in the device groups list until a group-level action is taken against that group.

What's New Since 10.79 Release Summary

Description of the latest new features and other information specific to the current release of IBM® MaaS360® Mobile Device Management (SaaS).

Version 10.79.cd.11112020 Released 11 November 2020

Deploying macOS updates to devices

MaaS360 now allows you to remotely deploy the latest security patches and macOS updates to devices from the MaaS360 Portal. For more information, see Deploying macOS updates to devices.

Version 10.79.cd.30102020 Released 30 October 2020

- MaaS360 adds localization support for the Security dashboard.

Version 10.79.cd.23102020 Released 23 October 2020

Support for business template based policies for Windows 10

MaaS360 provides a set of predefined policy templates that are based on common business use cases. When you create a policy, you can select an existing business use case as a base policy. For Windows MDM policies, MaaS360 now provides a set of predefined policy templates that are based on the following compliance business cases:

- AE8 (Australian Essential Eight)
- PCI (Payment Card Industry)
- HIPAA (Health Insurance Portability and Accountability Act)

You can modify the business template policy based on your organization's requirements. When you push this policy to Windows 10 devices, the MaaS360 policy recommendation engine suggests community usage statistics that you can apply to those devices if needed. For more information about using business template based policies, see Creating a business template based policy.

Version 10.79.cd.16102020 Released 16 October 2020

Enrollment screen string changes for macOS 11 or later versions

- MaaS360 enhances the strings on the macOS 11 (Big Sur) enrollment screens to provide a consistent enrollment experience across iOS, iPad, and macOS.

Version 10.79.cd.13102020 Released 13 October 2020

Improvements to the Windows 10 Bulk Provisioning Tool retry options

If you are using the Windows 10 Bulk Provisioning Tool to bulk enroll Windows 10 devices, it might take MaaS360 up to 2 hours to enroll those devices into the MaaS360 Portal.

-

10.79 Release Summary

iOS/macOS MDM

Enhancements to User Enrollment >>

In 10.78, MaaS360 added support for User Enrollment, a new mode of enrollment that is designed for employee-owned (BYOD) devices. For self enrollments, MaaS360 added corresponding device enrollment settings in the MaaS360 portal to define whether the BYOD devices should be enrolled via Managed or User Enrollment mode.

In this release, MaaS360 adds the following enhancements to User Enrollment:

- **Added Enroll using iOS User Enrollment checkbox to the Add Device workflow**

  Administrators can now choose User Enrollment as a device enrollment mode while creating an enrollment request through the **Devices > Enrollments > Add Device** workflow. The new **Enroll using iOS User Enrollment** checkbox is available by default to all customers. User Enrollment does not require administrators to pre-configure device enrollment settings prior to creating an enrollment request.

  Note: A user account with a valid Manage Apple ID is a pre-requisite for creating an enrollment request with User Enrollment. When the **Enroll using iOS User Enrollment** option is selected, **Device Ownership** defaults to **Employee** in the **Add Device** workflow.

- **Removed MaaS360 authentication prompt to simplify enrollment experience**

  In 10.78, as a part of device enrollment, MaaS360 displayed two authentication screens: MaaS360 user authentication (One Time Passcode, LDAP/AD, or local user) and Managed Apple ID. To provide a seamless enrollment experience, MaaS360 removes the additional layer of user authentication screen (One Time Passcode, LDAP/AD, or local user) that was displayed prior to downloading enrollment and configuration profiles, allowing users to complete the enrollment by just authenticating against their Managed Apple ID.

- **Supported apps for User Enrolled devices**

  MaaS360 supports the distribution of user-licensed VPP apps, enterprise apps, and web clips to User Enrollment devices. The device-licensed VPP apps and public iTunes apps are not supported.

Managed Apple ID features >>

- **Managed Apple ID is now an editable field in user summary page >>**

  The Managed Apple ID is now available as an editable field across all types of user records such as Active Directory, LDAP, Azure AD, and so on.

- **User's email address can now be used as Managed Apple ID >>**

  Administrators can now use the Email Address in the User Summary page as Managed Apple ID without having to separately input Managed Apple ID for each user. When the **Use Email Address as Managed Apple ID** setting in **User Settings** > **Basic** is selected, the email address of the user is automatically used as Managed Apple ID in the subsequent User Enrollment deployments even though the **Managed Apple ID** field in the User Summary page is blank. **Note**: This feature does not auto-populate the email address into the **Managed Apple ID** field in the User Summary page. It simply uses the email address instead.

View APNS certificate serial number in the MaaS360 portal >>

Administrators can now get their APNS certificate serial number directly in the MaaS360 portal without having to contact Support. The serial number can be used to determine the Apple ID that is used to set up the APNS certificate or change the Apple ID in scenarios where the Apple ID credential that was used for setting up the APNS certificate is no longer available.

Enhancements to the VPN and VPN on Demand settings in bulk edit of iOS policies >>

MaaS360 adds support to manage existing VPN and VPN on Demand profile configurations in the iOS policies that are chosen for bulk edit. These profiles are managed based on **VPN Host Name** and **VPN on Demand Rule Dictionary Name** that are considered as unique identifiers for VPN and VPN on Demand configurations across iOS policies.

- If multiple policies have the same VPN type and Host Name, the VPN configurations are superimposed with respect to the original policy. If the policies have the same VPN type and different Host Name, a new copy of VPN configuration is created in the selected policies.
- If multiple policies have same VPN on Demand Rule Directory Name, the VPN on Demand configurations are superimposed with respect to the original policy. If the policies have a different Rule Directory Name, a new copy of VPN on Demand is created in the selected policies.

Android

Block the App Catalog (Managed) apps on non-compliant devices >>

The apps distributed via App Catalog with the **Enforce Compliance** flag will now be blocked on non-compliant Android Enterprise devices. In the previous releases, instead of suspending the apps, MaaS360 displayed an overlay screen to block access to those apps. **Note**: Supported on Android 7.0+ devices. Requires MaaS360 for Android version 7.20 +.

Redesigned user interface and new enhancements for Kiosk mode >>

Kiosk mode gets a redesigned user interface for improved usability with an emphasis on cleaner and simpler design. MaaS360 also adds enhancements such as app action shortcuts and a 60-second countdown timer for the single-app mode.

Lock device to MaaS360 to resume Device Owner enrollments on reboot >>

To prevent users from skipping the device enrollment screens, MaaS360 adds support to lock the devices to MaaS360 until the enrollment is completed. The lock device action is issued to the devices as a part of Device Owner enrollment configuration in the form of key-value paris. When this setting is enabled, the MaaS360 app is automatically launched after the reboot and the enrollment will be resumed from where it left off. After successful enrollment, the lock is removed and users will be able to access the device. **Note**: Supported for DO enrollments: QR code, ZTE, and KME. Requires MaaS360 for Android version 7.20+.

Pass custom parameters to Device Owner enrollment configuration (JSON) file >>

In addition to the existing device provisioning options, MaaS360 now allows administrators to pass custom parameters to the enrollment configuration (JSON) file. Administrators can use the **Custom Attributes** field in the Android Enterprise QR code/ZTE/KME provisioning window to add up to 10 parameters in the form of key-value pairs. MaaS360 agent reads these parameters as a part of Device Owner enrollment and issues corresponding action to the device. In the previous releases, administrators had to manually add the parameters to the JSON file.

Added a new attribute to identify devices by their One Lock or Unified Password status >>

MaaS360 adds a new device attribute **One Lock Status** in **Device Summary** > **Security & Compliance** to make it easier for administrators to track the devices that have the same password enabled for both device and work profiles. Administrators can also use the advanced search to filter devices based on their unified password status.

Removal of ActiveSync configuration on selective wipe

The corporate ActiveSync accounts that are configured through policies will be automatically cleared from the device when the actions: *policy change*, *selective wipe*, and *reset corporate settings* are issued to the device. When the selective wipe action is taken, users must reconfigure those ActiveSync accounts. **Note**: Supported only on Android Enterprise (PO and DO) modes. Requires MaaS360 for Android agent 7.20+.

Samsung Knox Platform for Enterprise (KPE) activation is available for all customers >>

In the previous releases, KPE activation support was rolled out to new customers. Effective 10.79, KPE activation is available for all customers by default and the KPE key is automatically deployed and activated during the MaaS360 agent upgrade/enrollment.

Offline geofencing enhancements (beta)

In the previous releases, when the device was offline, MaaS360 applied the policy corresponding to the last known location if the GPS was turned on. In this release, MaaS360 automatically applies a checked-out policy to the device when the device goes offline. The checked-out policy is the policy on the device with higher precedence. **Note**: In MaaS360, the order of priority to decide which type of policy is applied on the device is as follows: compliance rule, location, group, device, user, default.

COPE end-of-life

MaaS360 marks COPE mode for end-of-life with MaaS360 for Android 7.20. As a result, MaaS360 does not support new COPE (Corporate-Owned, Personally Enabled) enrolments, and the configuration options to enroll a device in the COPE mode are removed from the MaaS360 portal. Administrators will have to regenerate any old configuration profiles QR codes/JSON files which have the COPE flag set to true.

Behavior on Android 10+ device when MaaS360 agent targets Android Q (10) APIs >>

Android 10 marks the official deprecation of Device Admin mode. As a result, some of the Device Admin policy features will no longer be supported on Android 10+ with the MaaS360 app version 7.20+.

Platform

Enhancements to the Search option in the MaaS360 portal home page >>

MaaS360 continues to enhance the user experience by revamping the search option in the portal home page to maintain consistency in the portal UI elements design and engaging digital interface. Along with the revamp of UI elements, enhancements are made in the search results as well. The current **show more results** option is renamed to **View more** in the search results. Click **View more** that directs you to the search results of respective

workflow page such as Devices, Users, Apps, and Docs. To view all rows in the search results, click **View more** that is displayed after 5 rows in the individual search results section.

Splitting of enrollment authentication screens >>

There are a number of authentication modes that are becoming popular in enterprise authentication. To support them and make the authentication experience seamless, MaaS360 has split the enrollment authentication page into two. The first page will get the username/email that helps to identify the authentication source for the device and 2nd screen will challenge for the password. In case of User Enrollment, there is no need for a password in the MaaS360 side as Apple does the authentication during the enrollment screen.

Provision to delete an Administrator account from MaaS360 portal >>

A new action called 'Delete' is introduced in the Administrators page, which is an extension of 'Deactivate' Administrator. In case of 'Deactivate' action, Administrator account is deactivated and anytime the account can be activated again. However, the usernames of deactivated Administrator account cannot be assigned to any other Administrator. To overcome this limitation, MaaS360 supports the permanent deletion of the Administrator account by using 'Delete' action. The username that is associated with the deleted Administrator account can now be allocated to any other Administrator. In the portal UI, the Deactivate and Delete actions are now available under the option 'Remove' in the Administrators page.

Using the Delete action, PII data that is associated with this Administrator is also deleted. When the Administrator account is deleted, the Administrator details are no longer shown in the Administrator grid. However, any actions that are performed by the Administrator in the past such as apps, policies, or device actions continue to show the Administrator details in the audit history page even if the Administrator account is deleted.

Limiting the display of user owned devices shown in the User Summary >>

The User Summary page displays device details for all active devices that are owned by the user. From this release, display of user owned devices in the Owned Devices section is restricted to show up to 10 active devices. For any user account that has more than 10 active devices, an option to **click here to view all devices** is displayed. On the click of this link, the page directs to search results in the **Advanced Search** that displays device details for all devices that are owned by the user.

App Management

Enterprise app support to Work Profile devices

Administrators can now deploy enterprise (corporate) apps to the Work Profile (PO) devices. After the deployment, administrators can also track the status of the app in the MaaS360 portal.

Delete all app reviews from the App Summary page >>

If employees provide inappropriate reviews for an app, administrators can now delete all the reviews for that app from the App Summary page.

App distribution architecture redesign

For the 10.79 platform release, all customers with a deployment size of 1,000 devices or less are moving to the new redesign of the app distribution architecture. All new customer accounts after the 10.77 platform release were already migrated to the latest redesign. No impact to customers is expected with the migration to the new architecture.

iOS App Auto Update Settings >>

iOS app store upgrade today has an option to enable/disable at the tenant level. Also, the admin can override the user's preference to get the app updates. MaaS360 has introduced a new updated auto-update feature to new customers. Now, this feature is going to be enabled for all customers batch by batch in Q4 2020.

Customers will see an option now to enable/disable auto-update for app store apps at the app level in addition to the tenant level settings. Customers can use this flag to test the app before the upgrade is pushed to all the devices. In addition, the tenant level settings are upgraded to have the following options:

- Administrator Controlled option will let the administrator device the upgrades that need to be pushed to the device. If this option is selected and app-level update is selected, only then the auto-update will be pushed to the device. By default, the app level update flag is enabled.
- The user-controlled option will let the end-users decide whether to receive the auto-update or not. The auto-update option in the end-user app catalog UI will show up only when this option is enabled. When this option is enabled, the administrator will not be able to choose to push updates. End-users' preference is taken into account here.
- Auto-update off will switch off all the auto-updates on the device.

Windows

Windows 10 Home device enrollment support >>

As more employees work remotely, organizations are experiencing an increase in the use of Windows Home edition in the enterprise. In addition to supporting Windows 10 (Education, Enterprise, Professional) devices in the MaaS360 Portal, MaaS360 now allows administrators to also enroll, manage, and support software distribution and OS patch management to Windows 10 Home devices.

MaaS360 adds a new Windows 10 device enrollment workflow that allows device users the option to enroll Windows 10 Home devices or Windows (Education, Enterprise, Professional) devices into the MaaS360 Portal after receiving the MaaS360 enrollment request URL notification that is sent by email or text message from an administrator.

Windows 10 Home devices are enrolled in the MaaS360 Portal in DTM mode, which uses traditional agent-based management that is normally used for Windows 7, while Windows 10 (Education, Enterprise, Professional) devices are enrolled in MDM mode, which uses modern management capabilities built on the Windows 10 MDM APIs.

Note:

- For new MaaS360 Portal accounts, make sure that you enable the **Laptop and Desktop Management** setting in the MaaS360 Portal at **Setup > Services**.
- For existing MaaS360 Portal accounts, this service is already enabled and you can start enrolling Windows 10 Home devices using DTM mode.
- For Windows 7 devices, contact IBM Support for assistance with enrolling Windows 7 devices in DTM mode.

TeamViewer unattended remote access support for Windows 10 devices >>

TeamViewer provides remote support (remote view and control) to managed devices from the MaaS360 Portal. The MaaS360 integration with TeamViewer allows you to view or control managed devices as a part of remote support sessions to troubleshoot device issues without needing to travel for in-person support.

Windows 10 devices are now supported for TeamViewer's unattended access mode of remote support. TeamViewer unattended access mode allows permanent access to remote devices without requiring end-user intervention. This feature is supported for Windows 10 MDM-managed devices only. This feature does not support Windows DTM-enrolled devices.

New Microsoft Defender Application Guard policy >>

MaaS360 adds support for Microsoft Defender Application Guard settings in the Windows MDM policy. Application Guard, a hardware-based endpoint defense, is a security tool that is built into Microsoft Edge. Application Guard isolates enterprise-defined untrusted sites from the desktop (host) in a virtual machine (VM) to prevent malicious activity from reaching the desktop. This feature is supported on Windows 10 version 1709 and later.

With this policy, if a user visits an untrusted site through the Edge browser, the browser opens that site in an isolated Hyper-V enabled container that is separate from the host machine. If the untrusted site that is in container isolation is a malicious site, the host machine is protected and the attacker cannot access enterprise data.

Application Guard works with the Group Policy where the administrator configures a setting once, and then copies that setting to many computers. For example, you can set up multiple security settings in a GPO, which is linked to a domain, and then apply all those settings to every computer in the domain.

Administrators can configure the following policy settings to manage the implementation of Application Guard for the organization:

- Clipboard behavior and content: Choose what copy and paste actions are allowed for text and images between the user's device and the Application Guard container.
- Printing from the container: Allows the user to print content (PDF files, XPS files, print from local printers, print from network printers) from the Application Guard container.
- Camera and microphone access in the container: Allows the Application Guard container to access a device's camera and microphone if those settings are also enabled on the user's device.
- Retain user-generated browser data: Saves user data (such as passwords, favorites, cookies) that is created during an Application Guard container browsing session.
- Graphics acceleration: Allows graphic-intensive sites to load video faster by accessing the virtual graphics processing unit or uses the device's CPU for graphics. This setting is supported on Windows 10 version 1803 and later.
- Download files to the host file system: Allows users to download files from the Application Guard container to the host operating system or keep files local on the device (does not download files to the host file system). This setting is supported on Windows 10 version 1803 and later.
- Block external content on enterprise sites: Blocks content from unapproved sites from loading or allows non-enterprise sites to open on the device. This setting is supported on Microsoft Edge on Windows 10 Enterprise or Windows 10 Education with Microsoft Defender Application Guard in Enterprise mode.
- Certificate thumbprints: Shares certain device-level root certificates with the Application Guard container. This setting is supported on Windows 10 version 1803 and later, Microsoft Edge on Windows 10 Enterprise, or Windows 10 Education with Microsoft Defender Application Guard in Enterprise mode.

ADMX-backed policy support in the Custom OMA Settings policy >>

MaaS360 provides a new workflow where administrators can use custom OMA XML configuration files as part of the Windows policy to push Group Policy administrative templates (ADMX-backed policies) to Windows 10 devices. This feature is supported on Windows 10 version 1703 and later.

An example is provided in the Knowledge Center topic Using the custom OMA settings policy to push ADMX-backed policies to Windows devices that explains how to use the Custom OMA settings policy to create the custom OMA XML configuration file for an ADMX-backed policy, upload that content to the MaaS360 Portal, and then push that policy to Windows 10 devices.

New patch management restart settings >>

MaaS360 adds functionality to the Patch Management workflow by allowing administrators to notify users that a restart is required on a user's device after an OS patch is applied to that device.

Device users are provided an option to either defer the device restart by a setting a specific amount of time (in minutes, hours, or days) in the MaaS360 Portal user interface or opt for the restart immediately. The administrator configures the threshold date for the device restart. Device users have the option to defer the restart multiple times until the threshold date is reached. This deferral provides the user with enough time to continue working and restarting the device at their convenience.

Enhancements to the Windows enterprise app installation success criteria during app upload >>

MaaS360 adds functionality to the Windows Enterprise App Installation workflow by providing new install criteria options that allow administrators to determine whether a script/job executed successfully on a Windows device. The new install criteria options allow administrators to check for the non-existence of certain registry keys, files, or processes or use exit codes to validate that the script/job executed successfully on the device. In previous releases, the administrator could only determine whether a script/job executed successfully on the device by checking the existence of certain registry keys, files, or processes.

MaaS360 has updated the **Relevance to install success criteria** setting during uploads of Enterprise App for Windows apps by providing the following new install criteria options to the administrator:

- Administrators can now enter negative install success/relevance criteria for Windows enterprise apps to determine whether an app was successfully uninstalled or removed from a device during an app upload.

The negative install success/relevance criteria includes the following:

- Registry key does not exist
- File does not exist
- Process not running

This criteria applies to the following app types:

- Windows Installers (.msi)
- Windows Executables (.exe)
- Windows Scripts (.bat, .vbs, .ps1, .reg, .py)

- Administrators can now enter exit code based install success criteria, as a numerical value or as a comma-separated list of numerical values, to determine whether an app was successfully uninstalled or removed from a device during an app upload.

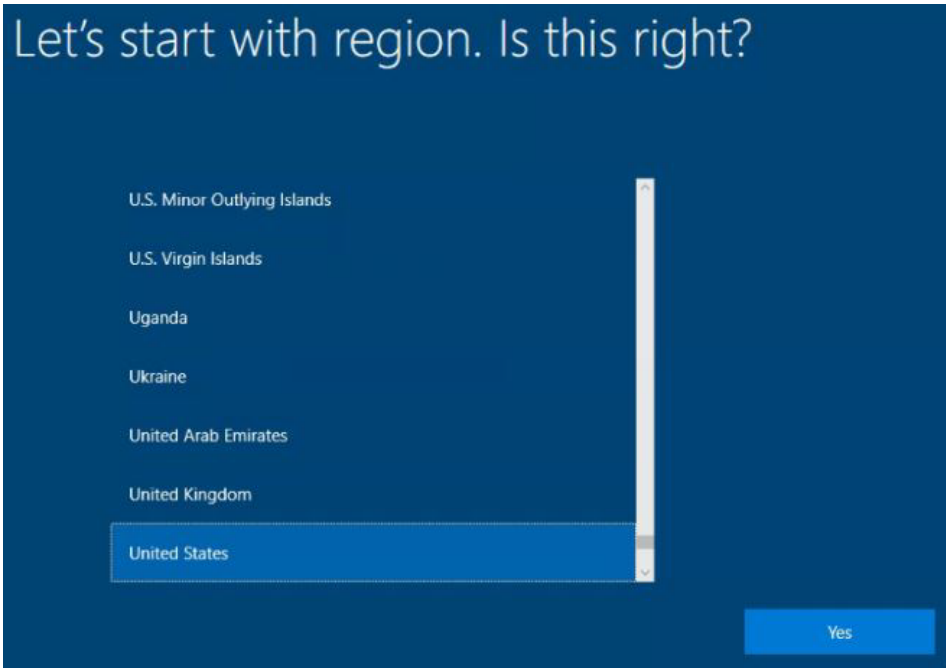
What's New Since 10.78 Release Summary

Description of the latest new features and other information specific to the current release of IBM® MaaS360® Mobile Device Management (SaaS).

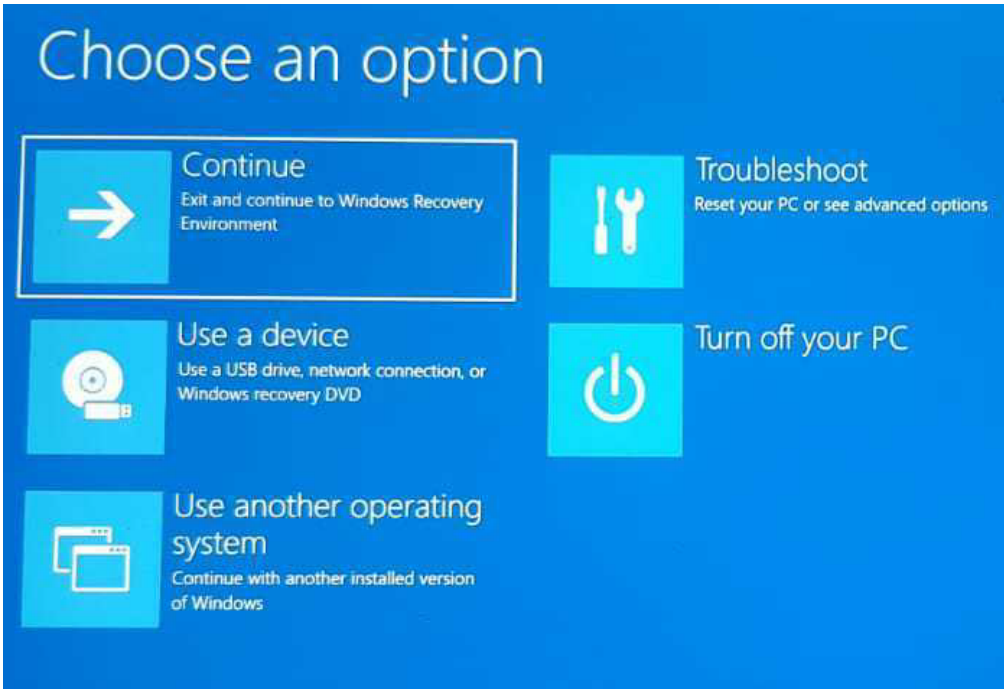
Version 10.78.cd.10072020 Released 10 July 2020

The **Wipe** device action on Windows 10 version 1709 and later is supported on MaaS360 through doWipeProtected. Unlike doWipe, which allows a device to circumvent the wipe action by making the device go through a power cycle, doWipeProtected continually tries to reset the device until the device is actually wiped.

When doWipeProtected is successful, the device is wiped remotely by the administrator, where all data is removed completely from the device's internal drive. After the device is completely wiped, the following screen is displayed to the administrator:



Note: If a device is encrypted, the **Wipe** device action could place that device in a state where the operating system is corrupt and the administrator cannot install or recover the operating system on the device. The following screen is displayed to the administrator after an encrypted device is wiped:



For more information on device actions, see Managing devices in the MaaS360 Device Inventory.

10.78 Release Summary

iOS/macOS MDM

User Enrollment Mode >>

Apple's Managed mode enrollment for employee-owned (BYOD) iOS and macOS devices, allows a number of device-level controls to the administrator such as factory reset, view device serial number, personal apps on employee device. These controls led to user data privacy concern. Apple's answer to solving this problem is the introduction of the **User Enrollment** mode to enroll employee-owned iOS and macOS devices. MaaS360 is supporting this new mode of enrollment on iOS 13+ non-supervised devices. With this capability, administrators can manage and protect only the corporate data on BYOD devices instead of complete management of employee-owned devices.

Android

Android 11 zero day support

With Android 11 zero day support, new devices will enroll with Android 11 and existing devices upgrading to Android 11 will continue to work. MaaS360 displays a redesigned location permission screen on Android 11 devices.

New user-less enrollment for Android Enterprise shared devices >>

MaaS360 adds support for new user-less enrollment allowing administrators to easily enroll Android Enterprise shared devices without attributing those devices to a specific user. MaaS360 skips user authentication during the enrollment and initially enrolls the device into MaaS360 in a signed-out state. While creating an enrollment configuration, all the user-specific fields are hidden when the Userless Enrollment option is selected.

Note: Supported only on Android Enterprise DO enrollment modes: Knox Mobile Enrollment, Zero-Touch Enrollment, and QR code enrollment.

Track managed app configuration feedback in App Catalog and device view >>

When administrators subscribe to app configuration feedback, MaaS360 tracks the status of the app configuration whenever configuration changes are applied to the app. The feedback can be a confirmation message that the configuration is successfully applied to the app or an error message if the app failed to apply the configuration. MaaS360 adds a new column **Managed Configuration** in the App Catalog and device view to track the app configuration feedback. **Note**: Applies to Android Enterprise PO and DO devices.

Redesigned Location screens in MaaS360 agent >>

MaaS360 redesigns the Locations screen for the Android agent to make it easier to view the list of pre-configured locations, grant permissions, track checked-in time and distance from the current location to other locations.

Enhancements to cross profile intent filter policy >>

MaaS360 supports cross-profile intent filters for Profile Owner enrollments. These intent filters allow intents from the work profile to access the personal profile or vice versa. In previous releases, with the limited attributes (Action, Category, and Mime Type), administrators could not declare intent filters for important tasks that involved attributes such as Scheme. For example, administrators could not define intents to allow a Google Chrome webpage opened in a personal profile to start Secure Mail in the work profile to send a mail with a mailto: URL, because the intent only contained data and no MIME type. Effective 10.78, MaaS360 adds new attributes (Scheme, Authority host, Authority port, Path, Scheme specific part) to allow administrators to define advanced intent filters. **Note**: Requires MaaS360 for Android agent 7.10+.

Samsung Knox license management >>

Samsung announced the deprecation of legacy ELM and KLM keys by the end of December 2020 in favor of the Knox Platform for Enterprise (KPE) key. Android Enterprise customers are recommended to switch to the Knox Platform for Enterprise (KPE) key with the Knox SDK at the earliest. MaaS360 adds support for three KPE license variants: **KPE Standard** (free), **KPE Premium** (paid), and **Backwards—compatible** key. As a part of device enrollment and the MaaS360 agent release, MaaS360 ensures that devices running Knox v2.7.1 and earlier receive the **Backwards—compatible** key, and devices with Knox v2.8 and later receive the **KPE Standard** key. However, administrators must configure the **KPE Premium** (paid) license key through **MDM policy > OEM Settings** to activate licenses on devices. The KPE Premium key overrides the existing license keys that are already activated on the device. MaaS360 also removes the **Configure Samsung Knox License for Samsung devices** field from the Device Enrollment Settings workflow to prevent administrators from activating legacy license keys.

New policy to restrict Google apps to allowed domains >>

MaaS360 now allows administrators to specify which domains are allowed to access Google services such as Mail and Play Store. When a set of domains are whitelisted, all other Gmail accounts such as personal accounts are automatically blocked. If your organization uses G-Suite and enabled G-Suite binding with MaaS360, this policy can be used to restrict play store access only to corporate Google accounts. For example, you can allow corporate domains such as mycompany.org so that personal accounts such as gmail.com are automatically blocked. If domains are not specified, users

can add and sign into Google services from any account. **Note**: Requires MaaS360 for Android agent 7.10+.

App wrapping support for apps compiled with the D8 compiler

In 10.77, MaaS360 added support for Android apps complied with the D8 complier. Effective 10.78, customers can wrap D8 complied apps without passing any parameters on the portal.

Track the status of configured Android Enterprise policy settings and device attributes

In consistent with MaaS360 Device Admin agent, the MaaS360 Android Enterprise agent now reports the status of configured policies: **Passcode Status**, **Configured Settings** (ActiveSync and VPN), **Failed Settings**, and **Camera Present** in the device summary > **Security and Compliance** page.

Multi-level folder structure for managed Chrome bookmarks >>

MaaS360 now allows administrators to organize managed Chrome bookmarks into folders and sub-folders. Administrators can use forward slash (/) to create nested folders. For example, Books/Fictional/Hobbit will create the bookmark named Hobbit inside the Fictional folder inside the Books folder.

Modern Authentication support for Exchange ActiveSync >>

Microsoft announced deprecation of basic authentication for multiple protocols including Exchange ActiveSync. It is recommended to switch to OAuth 2.0 token-based Modern Authentication to continue with these services. MaaS360 adds the **Authentication Mode** field in the ActiveSync policy settings to enable the use of Modern Authentication for Exchange ActiveSync. **Note**: Google does not support modern authentication. It is recommended to configure the Google account with G-Suite binding for mail, calendar and contacts access natively. To enable modern authentication for Exchange ActiveSync, navigate to Android MDM policy > **Android Enterprise Settings** > **ActiveSync** > **Authentication Mode** and then select **Modern**.

Platform

Local Administrator login settings for Federated Single Sign-on >>

The **Federated Single Sign-on (SSO)** configuration in the **Advanced Administrator settings** is redesigned for SAML Single Sign-On and Corporate User Directory. The focus is to allow existing Portal Local Administrator accounts to continue to log in to the MaaS360 portal by using their local credentials even when SSO is enabled. This change is effective for all new customer accounts that are created after the 10.78 release. For existing customer accounts, **Allow existing Administrators to use portal credentials as well** option is not displayed in the UI going forward. With respect to the saved Administrator setting on whether *'Allow existing Administrators to use portal credentials as well* option' was previously enabled or disabled, Local Administrators are either allowed or disallowed to log in to the portal by using their local credentials.

Improved ways to generate access keys for the Web Services API Authentication Token >>

MaaS360 eases the existing method to generate access keys for Web Services API by introducing **MaaS360 Web Services**, **App Access Key**, and **Cisco ISE Integration** access key types. Customers and partners can use any of these 3 types to generate access keys depending upon the details in hand and the type of access key to be generated. For example, if appID details are known, then customer or partner can use App Access Key type to generate the access key. Customers and partners can further use this generated access key to get an OAuth token for using the Web Services API.

Allow partners to move customer and partner accounts within a hierarchy

MaaS360 allows Partner Administrators to self-serve the movement of customer and partner accounts within their hierarchy. Only a Partner Administrator with the access right **Allow movements of accounts within hierarchy** can perform this action. The Primary Administrator can add this access right to the Partner Administrator by assigning this access right from the **Grant Access** Rights page during the Add Role or Edit Role workflow. The Partner Administrator can then see the Move action in the Accounts page that is listed for all customer and partner accounts in their hierarchy. Using this Move action, choose the New Parent Partner Account under which you want to move the account and confirm the move action.

Note: This capability is available only for Partner accounts. Customer accounts do not get an option to move accounts within their hierarchy.

App Management

App Approval workflow for iOS custom B2B apps

MaaS360 extends the app approval workflow to custom B2B apps. With this support, administrators can set up quality, security, and compliance checks before the B2B apps are promoted to the App Catalog. For more information on the App Approval workflow, see https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/pag_source/concepts/pag_apps_app_approval.htm

On demand app refresh support for iOS custom B2B apps

MaaS360 extends the manual app refresh support to iOS custom B2B apps. With this support, administrators can manually refresh app details to receive the latest app updates in about 5 - 10 minutes. Without app refresh, it takes up to 24 hours for MaaS360 to automatically fetch the latest app updates.

Windows

New Microsoft Defender Firewall Settings policy >>

MaaS360 adds support for Microsoft Defender Firewall settings in the Windows MDM policy. These settings allow administrators to configure Windows Defender Firewall global settings, per profile settings, and also configure a set of custom rules to be enforced on a device. Administrators can also manage non-domain devices, reducing the risk of network security threats across all systems connecting to the corporate network.

Enhancements to the Custom OMA settings policy >>

Windows 10 custom profiles use Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings to configure different features that are used by mobile device manufacturers to control features on a device.

The MaaS360 Custom OMA policy includes many built-in settings that allow you to control different features on devices in your organization. Use this policy when you want to use device settings and features that are not built in to the Windows MDM policy. The policy Help topic provides sample procedures on how to create and remove custom OMA (XML) files from devices. **Note:** This feature is intended for advanced administrators. Contact IBM Support to enable this feature.

Local file share support for Windows app distribution >>

MaaS360 adds functionality to the App Distribution workflow by allowing administrators to host Windows apps on a password-protected file share located on their organization's network.

In previous releases, the only option available to administrators for distributing Windows apps to devices was that the app publish process always uploaded the app binaries to a MaaS360 (content delivery server) CDN server, and as part of installation, these apps were downloaded by end users onto their devices from the MaaS360 CDN server.

In the 10.78 platform release, administrators can now host Windows app binaries locally on a password-protected file share on their network. The common credentials used to access the network share by the devices are provided as part of the publishing workflow. The devices that need to install these apps, access that file share with the credentials provided as part of publishing workflow and download the app binaries from the local share instead of from the CDN server. This functionality helps reduce internet bandwidth and increases the speed of installation and improves compliance across all devices.

Note:

- MaaS360 only supports EXE, MSI, and BAT files in the network share publish model.
- Windows Universal App Packages (APPX and APPXBUNDLE) are not supported in this model.
- Windows 7 devices managed by DTM are not supported in this model.
- The device that is receiving the app must be connected to the organization's network (VPN or intranet). If the device is not connected to the organization's network, app installation will fail on the device.

Unlock developer settings on Windows Universal App Packages >>

MaaS360 automatically configures some settings in the background on devices to successfully distribute and publish appx packages on devices. For example, for every appx app distribution, the 'Developer settings' for the device is changed to 'Sideload apps' on the device, which sideloads an app successfully. MaaS360 takes care of changing these settings during installation and once these appx apps are installed, the 'Developer settings' on the device revert back to the original settings.

Windows Phone end of support >>

Microsoft has ended support of Windows Phone (8.0, 8.1, 10), new Windows Phone OS builds, and the business app store. MaaS360 no longer allows new Windows Phone enrollments in the MaaS360 Portal. However, existing Windows Phone enrollments will continue to work in the Portal. The following settings were added or disabled for the 10.78 release onwards:

- A message explaining that MaaS360 does not support Windows Phone enrollments is displayed if a user tries to access the enrollment URL in the Windows Phone browser, or tries to add the MDM Profile directly from the phone at **Settings > Account > Access work or school**.
- On the **MaaS360 Portal > Setup > Services** page, the Upload Windows Phone Company Hub Certificate option to upload a new or renewed Symantec certificate for Windows Phone was removed from the Mobile Device Management section.
- The Windows Phone Symantec Certificate Expiration banner was removed from the My Alert Center section on the MaaS360 Portal Home page.
- The Windows Phone option was removed from **Setup > Settings > Device Enrollment Settings > Add Device > Advanced > Select Platform** drop-down list.
- The Windows Phone option was removed from **Setup > Settings > Device Enrollment Settings > Advanced > Enrollment Programs > Device Platforms allowed to enroll** section.

What's New Since 10.77 Release Summary

Description of the latest new features and other information specific to the current release of IBM® MaaS360® Mobile Device Management (SaaS).

Version 10.77.cd.29042020 Released 29 April 2020

Enable PIN Recovery parameter added to the existing Windows Hello for Business or Passport for Work workflow

MaaS360 provides the new Enable PIN Recovery setting for Windows Hello for Business or Passport for Work workflow. This setting is available on the Windows Hello for Business policy in the MaaS360 Portal at Security > (and then)Policies > (and then)Default Windows MDM Policy > (and then)Enterprise Settings > (and then)Windows Hello for Business. This setting allows an end user to reset their Hello for Business PIN using the Hello for Business PIN recovery service, without intervention from an administrator. For more information, see the Windows Hello for Business policy settings.

Version 10.77.cd.14042020 Released 14 April 2020

Enable EULA management from Services page

Administrators can now directly enable EULA Management from the Services page. Previously, MaaS360 support team had to enable this feature for customers on request. When enabled, it provides the ability to distribute Usage Policy via the WorkPlace persona policy.

Version 10.77.cd.14042020 Released 14 April 2020

Advanced iOS policies

MaaS360 adds support for the following iOS advanced policies:

- iOS policy > Restrictions > **Allow Deprecated Web KitTLS** – Apple dropped support for TLS 1.0 and 1.1 in iOS 13.4. If this policy is turned on, Safari does not allow accessing websites that use TLS 1.0 and 1.1. Supported on iOS 13.4 and later.
- iOS policy > Supervised Settings > **Allow Shared Device Temporary Session** – If this policy is turned off, guest login sessions are unavailable on Shared iPad devices. Supported on iOS 13.4 and later. For more information on Shared iPad temporary sessions, see https://support.apple.com/en-in/guide/mdm/cad7e2e0cf56/1/web/1#mdm6e1d78ad8

Version 10.77.cd.03042020 Released 03 April 2020

Support to track devices outside home country

MaaS360 adds a new tab **Outside Home Country** to the network overview report, making it easier for the administrators to track devices that are currently outside of their home country. This report can be used to support your organization's efforts towards ensuring safety of employees during the current pandemic. Administrators can also use the new **Devices outside their home country** My Advisor insight to navigate directly to the report from the home page.

Note:

- Home country is determined based on the country in which the user activated the device and has no relation to user's physical location.
- The feature is applicable only for cellular enabled devices.
- The network overview report is refreshed on daily basis.

Version 10.77.cd.02042020 Released 02 April 2020

MaaS360 DEP enrollment customization

Apple DEP customization: For iOS 13 and macOS 10.15 devices, Apple announces a new capability called DEP workflow customization. This feature allows enterprises to use their own web interfaces to customize their business needs for a number of use cases. With this customization, enterprises can now define their own user interface during device boot up.

How the Apple DEP customization works with the MaaS360 DEP enrollment: With Apple extending the support of DEP customization, MaaS360

now enhances two-factor authentication and SAML-based authentication to authenticate users during DEP device enrollment. This customization is supported on iOS 13 or macOS 10.15 and later devices. The DEP customization allows you to view more web user interfaces for user authentication during DEP enrollment. MaaS360 provides a new user interface that is based on the type of user authentication method that you selected in the device enrollment settings. For more information about two-factor authentication and SAML-based authentication, see Enrolling DEP devices using two-factor authentication and Enrolling DEP devices using SAML-based authentication.

Corporate Usage Policy enhancements: MaaS360 also enhanced the Corporate Usage Policy (CUP) for DEP device enrollment on iOS 13 and macOS 10.15 devices. Use this policy to customize the EULA policy (Acceptance Usage Policy) that you want users to view and accept during DEP device enrollment. For more information, see Applying the Corporate Usage Policy to DEP devices. This customization provides a unified enrollment experience, where the user authentication method during device enrollment is unified across all device platforms (Android, iOS, macOS, Windows). This unified enrollment also includes DEP devices for iOS 13 and macOS 10.15. For more information, see MaaS360 DEP enrollment customization use case.

10.77 Release Summary

iOS/macOS MDM

End of support for devices that use iOS 10 or lower version

MaaS360 always supports the last 3 versions of the iOS and macOS Operating Systems. Hence, we are dropping the support for iOS 10 and macOS 10.12 (Sierra) from this release. Any Operating System related issues or bugs for this version of the OS might not be fixed and we encourage customers to upgrade the OS to the latest or the supported versions. We suggest customers to use the latest OS version to make sure the features we provide can be experienced at best and the device is secure.

Android

Bulk enrollment support for device account based Device Owner enrollments >>

MaaS360 supports two account types: user account and device account for Android Enterprise enrollments. In the previous releases, MaaS360 restricted the number of enrollments allowed per device account to 1 device. In this release, MaaS360 removes the restriction to allow hundreds of devices to be enrolled per device account.

Note: Bulk enrollment is applicable only to device account type Device Owner enrollments: QR code, Zero-touch, and Knox Mobile Enrollment program. Google limits the number of devices that can be enrolled per user account to 10 devices.

Location permission requirements on Android 10+ devices >>

With the new permission changes in Android 10, users are required to turn on location service and grant location permission to MaaS360 app so the app can display configured SSID in Corporate Settings in MaaS360 agent and report last connected SSID to portal.

MaaS360 Kiosk app requires location permission to display configured Wi-Fi networks and Bluetooth devices in close range. The devices cannot discover Wi-Fi networks and Bluetooth devices until the location service is turned on.

Note: If the permission is blocked due to policy, the user will not be able to turn on the location service on the device.

Assign asset number as device name >>

MaaS360 adds a new option **Prompt for Asset Number** in the DO enrollment workflows, allowing the admin/user who is provisioning MaaS360 on device to assign an asset number as a custom device name. For more information on assigning a custom device name, see Assigning custom device name in MaaS360.

Note: Applicable to device account type Device Owner enrollments: QR code, Zero-touch, and Knox Mobile Enrollment program. This option is selected by default when using device account based enrollment.

Reduce the size of inline and attached images in Secure Mail >>

MaaS360 adds support to limit the size of the inline images and picture attachments that are uploaded to Secure Mail. When users upload a picture that exceeds the maximum inline or attachment limit, MaaS360 displays options (Original, Small, or Medium) that allow them to reduce the size.

Note: When the image size is scaled down, the resolution is also reduced when the image arrives at the destination.

Notification badge support for MaaS360 Secure Container apps >>

In the previous releases, MaaS360 added notification badge support for all third-party apps in Kiosk launcher. In this release, MaaS360 extends the notification badge support to MaaS360 Secure Container apps in Kiosk mode. Users can turn the badge notifications on/off through Kiosk settings.

Open/share third-party app data using Secure Editor and Docs >>

In the previous releases, MaaS360 restricted the use of Secure Container apps to access corporate content. In this release, MaaS360 removes the restriction to allow files from third-party apps to be opened and shared with Secure Viewer/Editor and MaaS360 Docs respectively. MaaS360 Viewer/Editor and Docs app work as shared resources in an Android Enterprise enrolled device. For example, users can now edit a Word document in the Files app with Secure Editor and then Share it to Docs app. When a supported file type is opened, Secure Editor/Secure Viewer is shown in **Open with** menu and MaaS360 Docs is shown in **Share via** menu.

Note: Applicable to Android Enterprise devices. Requires MaaS360 for Android 7.0. In Profile Owner mode, the files in Personal profile cannot be opened/shared with with Secure Container apps.

[Enforce device lock-down on devices that escape Device Owner enrollment >>]

To discourage skipping of Device Owner enrollment, MaaS360 restricts important features on the device until the device is completely enrolled. When users skip Device Owner enrollment at any stage after MaaS360 app is installed (or activated) as Device Owner, MaaS360 enforces following restrictions on the device:

- Account management: Users cannot access Play Store, add, or delete personal accounts such as GMail.
- App management: Users cannot uninstall or install apps from Play Store and or from other sources such as Android Debug Bridge (ADB).

Updated Device Enrollment Mode values in Device Summary for Android Enterprise devices >>

In the previous releases, MaaS360 displayed inaccurate values for Device Enrollment Mode attribute in the Device Summary page. 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.

MaaS360 will be rolling out the change to read the right values 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. Hence, **Container type** attribute will be used (instead of **Enrollment Mode**) in Device Summary page and in Advanced Search workflow to filter Device Administrator, Device Owner and Profile Owner devices using *Hardware Inventory* > *Container Type* selection.

MaaS360 also fixes the behavior on legacy Device admin enrollments, where Enrollment Mode was always **Manual**. You will start to see **Android Configurator** where applicable.

MaaS360 introduces **Container Type** attribute for Device Admin devices which will read accurate values such as **Device Administrator**, **Samsung Device Administrator**, **Honeywell Device Administrator**, **Bluebird Device Administrator**, etc, where OEM SDK is integrated.

Note:

- These changes are scheduled for a patch release on the platform post 10.77 portal release.
- Customers who are using Device Enrollment Mode attribute in device groups and home page watch lists to track and group Device Owner and Profile Owner devices will be automatically migrated to Container Type. The policy/rule assignments and application/document distributions will remain intact with this migration.
- 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+.
- 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 is not available already, so the device summary and smart search will show **Device Enrollment Mode** attribute value as **Not Available** after the change.

Updated X-Force categories used for URL filtering >>

MaaS360 adds the following new categories for Secure Browser category based URL filtering policies:

- Cities/Regions/Countries; Environment/Climate/Pets; Abortion; Early Warning; Crypto Mining

MaaS360 removes the following categories from Unknown:

- Cities/Regions/Countries; Environment/Climate/Pets

Note: Administrators are recommended to edit/make changes to URL filtering policies on Secure Browser policies within Persona Policies as desired to support such URLs that may fall out of Unknown categories now. For example, if you have blocked all **Unknown** categories, and will want to allow access to Cities/Regions/Countries, you can add them to whitelist now.

App Management

Manual refresh support for Google Play Private Channel apps >>

MaaS360 adds a new option **Refresh App Details** in App Summary page to allow administrators to manually refresh private channel app details. With this support, when an update is available in the Managed Play Store, the app description, version, and icon are reflected in App Summary page near real-time or within a maximum of 4 hours. In the previous releases, it took a maximum of 7 days to receive latest app updates.

Note: Supported only on Android Enterprise apps.

Distribute apps at device level for user accounts >>

MaaS360 adds support to distribute apps at device level through Managed Google Play. In the previous releases, with the user-level distribution, when a device moved out of a group, the app distribution on other devices in that group with the same user was removed. In this release, with the device-level distribution, MaaS360 only removes apps from the device fallen out of the group so that it does not impact the devices with the same

user that are already in the group.

Note: Requires MaaS360 for Android agent 7.0. Supported only for Android Enterprise apps.

App wrapping support for apps compiled on D8 compiler

MaaS360 adds support for Android apps complied on D8 complier.

Note: This feature is in beta and ***disableD8Check*** parameter must be set to ***true*** in App Configuration during wrapping.

App wrapping enhancements >>

- When large number of methods are detected, MaaS360 splits the methods into primary and secondary dex files. In the previous releases, MaaS360 displayed an option for administrators to move classes from secondary dex to primary dex just in case if some crucial classes were accidentally moved to secondary dex file. Effective 10.77, MaaS360 removes that additional step as MaaS360 automatically retains crucial classes in the primary dex file and moves other files to secondary dex file. Customers who want to use that option can set ***continueSplitDex*** parameter to ***false***.
- MaaS360 uses apksigner tool instead of jarsigner to sign APK files. **Note**: The APK signature will be invalidated if you make changes to APK after signing an app with apksigner.

Platform

Quick Start Setup Enhancements in the MaaS360 portal >>

From this release, setting up your MaaS360 account gets easy with the enhanced Quick Start setup wizard. With continuous focus on improving the portal experience, we have made enhancements to the Quick Setup. The wizard serves as guided walk-through to get all the information that you need to set up your MaaS360 account. Throughout the Quick Start setup, we recommend steps to perform that will help you complete the setup quickly. There are also additional error checks, help text, and links to documentation to help you complete each setup successfully. There are also additional notes on what happens if you skip any of the Quick Start setups. These notes help you make well informed decision if you want to skip any of the Quick Start setups or perform the setup right away.

Enable auto creation of end users on SAML authentication >>

MaaS360 supports creation of users account automatically in the MaaS360 portal during SAML based authentication for a user account that does not exist already in the portal. The user account that is added is listed under Users page in the portal. To support this function, enable the new setting **Enable auto creation of users on SAML authentication** that is added under **Device Enrollment Settings** > **Basic** settings in the **Authenticate using SAML** section. This capability is supported for DEP enrollments of iOS 13 and macOS 10.15 devices, Android, and Windows 10+ devices.

The SAML payload is standardized with mandatory user fields such as username, email, and domain fields for auto creation of users in cases where the user account is not existing in the portal already. If any of these mandatory parameters are missing or invalid during the device enrollment, then the following message is displayed, "The SAML token response is missing mandatory parameters or they are invalid. Please contact your IT administrator for further assistance. The parameters that are missing or invalid are: Domain, Email."

New OS Version (Numeric) search attribute in the Advanced Search >>

The Advanced Search conditions in the MaaS360 portal support new search attribute **OS Version (Numeric)**, a search based on Operating System condition. The previous attribute is now renamed as **OS Version (Numeric) Deprecated** and in this release, you see both these attributes that are listed under the Advanced Search based on Operating System. The **OS Version (Numeric)** allows advanced search based on OS version for any device platform, supports **OR** and **Advanced** search criteria. The existing attribute is renamed as **OS Version (Numeric) Deprecated** and any groups that are created based on this attribute continues to exist as before with the changed name. In future releases, the **OS Version (Numeric) Deprecated** will be removed and groups that are created by using the existing OS Version (Numeric) will be replaced with the new OS Version (Numeric).

Granular search condition on Settings Failure Reason attribute in the Advanced Search >>

The Advanced Search conditions in the MaaS360 portal support granular search conditions on **Settings Failure Reason** search attribute on **Security and Compliance** condition. With this search, you can now set Security and Compliance groups based on configured settings for the following search criteria: contains, begins with, does not contain, ends with, equal to, and not equal to.

Windows

Enhancements to the patch management workflow >>

For this release, MaaS360 added new capabilities to the granular patch management workflow that was released in 10.76. These new capabilities increase the granularity in this release such as scheduling when the patch management workflow starts, pushing multiple patches across multiple devices, stopping patch distribution at any time, and viewing the status of the patch distributions.

New policy settings added to the Update management settings policy for scheduling quality and feature updates >>

The Update management settings policy now includes many new settings:

- Allows administrators to configure service channels that specify when and how Windows devices receive quality and feature updates.
- Settings for rolling back both feature and quality updates.
- Allows administrators to schedule when not to actively patch devices.
- Specify which drivers are updated for quality updates.
- Specify the restart prompt duration to the user in terms of minutes.

New Windows Defender policy settings added to the Antivirus settings policy >>

The Antivirus settings policy provides multiple new settings that enable administrators to strengthen the security posture of their organization. These settings include attack surface reduction rules, which are a set of 15+ rules that ensure that endpoints are configured granularly to avoid any attacks. The following new settings were introduced in this release:

Under customizing scan settings and frequencies:

- Catch up full scan: Select to force Windows Defender to run a full scan after a scheduled scan was missed.
- Catch up quick scan: Select to force Windows Defender to run a quick scan after a scheduled scan was missed.
- Low CPU priority while scanning: Specify that Windows Defender uses low CPU priority for scheduled scans.
- Check for signature before running scan: Select that Windows Defender checks for new virus and spyware definitions before running a scan.
- Signature update fallback order: Select the order that definition update sources are contacted by Windows Defender.

Under advanced settings:

- Cloud block level: Specify how aggressive the Windows Defender antivirus engine is if it detects and identifies suspicious files. The following blocking levels are supported:
  - Default: The default Windows Defender blocking level that provides strong detection without increasing the risk of detecting legitimate files.
  - High: This blocking level aggressively blocks unknown files while optimizing client performance (increases the risk of false positives).
  - High +: This blocking level aggressively blocks unknown files and applies additional protection measures (might impact client performance and increase the risk of false positives).
  - Zero tolerance: This blocking level blocks all unknown executables.
- Cloud extended timeout: Specifies the number of seconds that the Cloud Protection Service blocks a file while the service checks whether the file is known to be malicious.
- Allow intrusion prevention: Enable this option to protect computers against known network exploits by inspecting network traffic and blocking any suspicious activity.
- Allow script scanning: Enable this option if you want to scan any scripts that run on computers for suspicious activity.
- Enable controlled folder access: Enable this option to protect documents and files from being modified by suspicious or malicious apps. This option helps protect documents and files from ransomware that can attempt to encrypt files and hold the files hostage.
- Applications allowed for controlled access to folders: Specify the apps that can access documents and files in the protected folders. These apps are included on a list of trusted software. If the app is not on the list, the controlled folder access blocks the app from making changes to files in the protected folders.
- Protected folders for controller folder access: Specify the folders that are protected from malicious apps or threats, such as ransomware. This feature checks against a list of known, trusted apps.
- Potentially unwanted application protection: Potential Unwanted Applications (PUA) is a threat classification based on reputation and research-driven identification. These apps are unwanted app bundles or their bundled apps. If you enable this option, PUA are blocked from downloading and installing on devices. You can exclude specific files or folders to meet the specific needs of your organization.
- Enable network protection: Allows you to prevent users and apps from accessing malicious websites. Set one of the following values:
  - Enabled: Protects employees from phishing scams, exploit-hosting sites, and malicious content on the internet.
  - Disabled: Allows connections to all websites without any protection.
  - Audit: Does not prevent users and apps from connecting to malicious sites, but does track their activities on those sites.

Under attack surface reduction rules:

- Attack surface reduction rules: Attack surface reduction rules target behaviors that malware and malicious apps use to infect computers with malicious code including:
  - Executable files and scripts used in Office apps or email programs that attempt to download or run files
  - Obfuscated or other suspicious scripts
  - Behaviors that apps would not normally initiate during normal business hours

New Windows 10 DTM-enrolled devices to Windows MDM migration workflow >>

Many of our customers still use Windows 10 devices that are enrolled in DTM mode, which is a traditional agent-based management that is best suited for Windows 7. The MaaS360 team has been investing more effort and time on building modern management capabilities recently. Customers can leverage these modern management capabilities built on the MDM APIs, natively provided by the Windows 10 OS. These

capabilities include over-the-air enrollments and management, security policies and restrictions, profiles push such as VPN, Wi-Fi, ActiveSync, and integration with Azure AD for Office 365 online roll out.

The OS Upgrade and patch management based on the MS Update Management workflows are also available. There are multiple other capabilities that MaaS360 supports on modern management.

For this release, MaaS360 introduces a migration workflow that allows administrators to seamlessly move Windows 10 devices off of DTM to MDM mode. Documentation is provided that covers the migration workflows, different scenarios that customers, and the steps to navigate those scenarios.

Windows 10 Onboarding Agent is now GA >>

Starting with the 10.77 release, the onboarding agent tool that is used for bulk provisioning of multiple Windows 10 devices at a time is generally available.

Windows Autopilot is now GA >>

In addition to OOBE settings and enrollment, the enrollment section now covers Autopilot. Currently, user driven enrollment is supported. Autopilot support is now available in MaaS360. The user interface covers Autopilot so that customers can start leveraging the feature.

Analytics

Improved UI design for Network, Browser Violation, and Mobile Expense Management reports >>

In this release, MaaS360 extends improved UI experience for Reports. The Network, Browser Violations, and Mobile Expense Management reports support new UI experience in this release. The reporting functions remains the same and only the UI design elements are changed. These reporting on the old UI in the MaaS360 portal continues to be accessible. To get access to the new UI reporting capability, contact IBM MaaS360 Customer Support team. Once the feature is enabled, customers can subscribe to these reports from the **MaaS360 portal** > **Setup** > **Settings** > **Administrator Settings** > **Analytics**.

Each of these reports also offer a detailed report view that comprises of chart data and table data. In chart data, you can view reports in the form of graph such as Bar chart, Pie chart, Line chart, and Area chart. In the table data, you can view device and network details such as the device name, user name, platform, home carrier, current carrier, and so on. These details are displayed as column headers in the table data along with an option to apply filters as needed.

For more information on ***report subscription, UI reporting settings***, and detailed reports in the expanded view, see Improved UI design for reporting**.**

Android Release Summaries

Release information for MaaS360 Android applications

Android 7.30 Release Summary

MaaS360 makes the Android app version 7.30 beta available on Play Store on 02 December 2020.

Work profile on corporate-owned devices (WPCO) >>

Work Profile is a secure container that separates work apps and data from personal apps and data while maintaining user privacy. In the previous releases, Work Profile could only be set up on personal (BYOD) devices that are also used for work. With Android 11, the Work Profile capabilities - privacy protections, securing and separating work data are extended from employee-owned devices to corporate-owned devices. With this support, employees can securely use company-owned devices for personal activities without sacrificing privacy. Administrators have more device-level control in WPCO scenario as compared to that offered for Work Profile on Personally-Owned devices. For example, administrators can wipe the entire device and disallow app installations from unknown sources on the personal profile of the device.

New group and device-level actions for Bluebird and Zebra devices enrolled in DO mode >>

MaaS360 now extends the Bluebird and Zebra group and device-level actions to Device Owner (DO) mode. With this support, administrators can remotely issue real-time actions such as push profile and push custom XML, and group-level actions such as copy file and push OS upgrade. In the previous releases, these actions were supported only on Device Admin devices.

New group-level action to reboot devices >>

MaaS360 adds a new group-level action to allow administrators to remotely restart multiple devices at once. Supported only on Android (DO) devices. Note: The users are not notified of the restart in advance, so any work the users are on will be lost.

Disabled location tracking on PO devices >>

In the previous releases, the location permission was auto-granted to the MaaS360 app when Android 11 devices were enrolled in Profile Owner (PO) mode, and end-users could not revoke the location permission from MaaS360 Settings. Effective 10.80, MaaS360 does not auto-grant location permission during the enrollment and ensures that the permission is only granted when geofencing is enabled. **Impact**: When the location permission is not granted, the MaaS360 app cannot report the last connected SSID to the MaaS360 portal.

Support for new Android Enterprise keyguard policies >>

MaaS360 adds new Android Enterprise policies to remotely control the Keyguard features: Face recognition and IRIS recognition. **Note**: Supported on Android 9.0+ (PO and DO) devices.

Cross profile communication between apps >>

By default, MaaS360 does not allow communication between apps across profiles. For example, the Google Chrome app in the Personal profile cannot communicate with its instance in the Work Profile. MaaS360 now allows administrators to use the security policy **Allow cross-profile apps** to configure apps that support cross-profile communication. **Note**: Supported only on Android 11+ devices that are enrolled in PO mode.

Package delegation support for Android Enterprise apps >>

As a Profile Owner or Device Owner, the MaaS360 for Android app can now grant certain delegations to other apps. Delegated apps are apps that receive additional permissions such as installing existing packages, enabling system apps, etc, from the profile owner or device owner apps.

Display work events in personal calendar >>

With cross-profile calendar support, administrators can use the security policy **Allow work events on personal calendar** to allow the personal calendar to show events from the selected work profile apps. **Note**: Supported on Android 10+ devices enrolled in PO mode.

Support to collect preboot security logs for DO and WPCO devices >>

MaaS360 adds a new Android Enterprise policy **Enable Enterprise Security Logging** to allow administrators to track preboot security logs from Device Owner (DO) and Work Profile on Corporate Owned (WPCO) devices.

Added Samsung system apps to list of apps that are allowed by default on enrolled devices >>

MaaS360 now adds a set of Samsung system apps that administrators can configure to be included by default on enrolled PO and DO devices. To select Samsung apps, navigate to Android policy > **Android Enterprise Settings** > **App Complaince** > **Configure allowed system apps**. In the previous releases, Samsung apps had to be manually added as additional apps in the MaaS360 portal.

Branding support for PO enrollment screens >>

Effective MaaS360 for Android 7.30 release branding is supported fully for Work Profile mode. In the previous releases, branding was supported only for

Container creation UI. In this release, MaaS360 extends branding support to all the enrolment screens for Work Profile mode and DA to PO migration screens.

Block remote images for external domain emails >>

MaaS360 adds support to block remote URL referenced embedded images in emails that are received from external domains. MaaS360 prevents the auto-download of remote images in Inbox, Sent, Draft folders, and reply, reply all, and forward options. This feature is applicable to primary, secondary, and delegation accounts. Administrators can use new security policies to define which emails can be classified as external emails.

Android 7.20/7.21 Release Summary

MaaS360 makes the Android app version 7.20/7.21 available in Play Store on 14 September 2020.

****Notice - there is dual versioning for this app (some clients may have 7.20 and others will only see 7.21) due to a code fix for the kiosk agent. Kiosk was fixed and the versioning updated before the affected code was distributed to clients.**

Landscape mode for passcode screen on tablets

When the screen orientation of Android tablets is set to landscape mode, the passcode screen of MaaS360 and SDK wrapped apps will also be presented in the landscape mode, instead of flipping to the portrait mode.

Redesigned user interface and new enhancements for Kiosk mode >>

Kiosk mode gets a redesigned user interface for improved usability with an emphasis on cleaner and simpler design. MaaS360 also adds enhancements such as app action shortcuts and a 60-second countdown timer for the single-app mode.

Lock device to MaaS360 to resume Device Owner enrollments on reboot >>

To prevent users from skipping the device enrollment screens, MaaS360 adds support to lock the devices to MaaS360 until the enrollment is completed. The lock device action is issued to the devices as a part of Device Owner enrollment configuration in the form of key-value paris. When this setting is enabled, the MaaS360 app is automatically launched after the reboot and the enrollment will be resumed from where it left off. After successful enrollment, the lock is removed and users will be able to access the device. **Note**: Supported for DO enrollments: QR code, ZTE, and KME. Requires MaaS360 for Android version 7.20+.

Enterprise app support to Work Profile devices

Administrators can now deploy enterprise (corporate) apps to the Work Profile (PO) devices. After the deployment, administrators can also track the status of the app in the MaaS360 portal.

Block the App Catalog (Managed) apps on non-compliant devices >>

The apps distributed via App Catalog with the **Enforce Compliance** flag will now be blocked on non-compliant Android Enterprise devices. In the previous releases, instead of suspending the apps, MaaS360 displayed an overlay screen to block access to those apps. **Note**: Supported on Android 7.0+ devices. Requires MaaS360 for Android version 7.20 +.

Microsoft RMS SDK upgrade from version 4.2.4 to 4.2.6

Microsoft announced the deprecation of older versions of Microsoft Rights Management Service (RMS) SDK and made the use of the latest RMS SDK platforms mandatory for all applications. In this release, MaaS360 adds support for the latest Microsoft RMS SDK. Users must upgrade Secure Mail, Viewer, and Editor apps to version 7.20 to continue to use the RMS-protected files in the MaaS360 app.

Join and Dial support for more conference tools >>

In addition to Webex and GoToMeeting, MaaS360 adds support for new conferencing tools: Zoom, Microsoft Teams, Google Meet, BlueJeans, StarLeaf, and Join.me. When users create or receive a meeting request, MaaS360 automatically displays **Join** and **Dial** buttons for the supported conferencing tools. MaaS360 also allows administrators to configure the list of custom URLs in persona policies to auto-recognize those meeting URLs in MaaS360 Calendar.

Removal of ActiveSync configuration on selective wipe

The corporate ActiveSync accounts that are configured through policies will be automatically cleared from the device when the actions: *policy change*, *selective wipe*, and *reset corporate settings* are issued to the device. When the selective wipe action is taken, users must reconfigure those ActiveSync accounts. Note: Supported only on Android Enterprise (PO and DO) modes. Requires MaaS360 for Android agent 7.20+.

New custom URI scheme to launch Secure Mail compose screen >>

MaaS360 adds support for a new custom URI scheme that can be used to launch the Secure Mail compose screen with pre-filled attributes: ***to***, ***cc***, ***bcc***, ***subject***, and ***body***.

Defect fixes

Defect #	Summary

Defect #	Summary
40057	In the previous versions, MaaS360 did not support custom URL Scheme for compose email.
39646	When the screen orientation of Android tablets was set to landscape mode, the passcode screen of MaaS360 and SDK wrapped apps were displayed in the portrait mode by default.
40088	In the previous versions, MaaS360 Browser did not support the **Accept** header in the download request. As a result, users could not download the files that were publicly available on third-party websites.
40973	The corporate support email in Settings > Corporate Support was truncated if the email had more than 30 characters.
40435	E-Fota agent failed to install on Samsung devices running Android 10 as a part of KME (Knox Mobile Enrollment) + Device Owner enrollment.
40515	The KME + DO enrollment failed as the Samsung Knox Platform for Enterprise (KPE) licenses could not be activated on devices that do not support Knox.
40607	When the Kiosk mode is enabled, the notification badges were not shown for the Messages app that was outside of the MaaS360 container.
40892	Contacts were not synced in Secure Mail and MaaS Contacts for delegated account
39454	The approved apps marked for **Install Automatically** were stuck in **Install Pending** state.
40596	The status of the identity certificate was shown **Pending** even though the certificate was successfully installed.
40521	In the previous releases, Device Owner enrollments did not resume after the device reboot.
40214	The QR code enrollments failed on Alcatel devices.

Android 7.10 Release Summary

MaaS360 makes the Android app version 7.10 beta available in Play Store on 16 June 2020.

Redesigned Location screens in MaaS360 agent >>

MaaS360 redesigns the Location screens for the Android agent to make it easier to view the list of pre-configured locations, grant permissions, track checked-in time and distance from the current location to other locations.

Android 11 zero day support

With Android 11 zero day support, new devices will enroll with Android 11 and existing devices upgrading to Android 11 will continue to work. MaaS360 displays a redesigned location permission screen on Android 11 devices.

Use camera and microphone for sites in Secure Browser >>

MaaS360 users can now share device's camera and microphone with sites in Secure Browser for features such as voice calls and QR code scan. When a site requests microphone or camera permissions, Secure Browser displays a prompt asking users to allow or deny those permissions. **Note**: Requires Secure Browser 7.10+ and MaaS360 for Android agent 7.10+.

View identity certificates deployed to devices in MaaS360 agent >>

When identity certificates (VPN, WiFi, Active sync, etc) are deployed to devices through MDM or Persona policies, users can now view the available certificates and their details in MaaS360 Settings > My Device > Identity Certificate.

Note: Supported on both Device Admin and Android Enterprise devices. Requires MaaS360 for Android 7.10 and later.

App wrapping support for apps compiled on D8 compiler

In 10.77, MaaS360 added support for Android apps complied on D8 complier. Effective 10.78, customers will be able to wrap D8 complied apps without passing any parameters on portal.

Track the status of configured Android Enterprise policy settings and device attributes

In consistent with MaaS360 Device Admin agent, the MaaS360 Android Enterprise agent now reports the status of configured policies: **Passcode Status**, **Configured Settings** (ActiveSync and VPN), **Failed Settings**, and **Camera Present** in the device summary > **Security and Compliance** page.

Collect and share Android bug report >>

In addition to device logs, MaaS360 now supports collection of Android bug report to allow the support team to easily identity and troubleshoot the bugs in the MaaS360 app. While sending device logs, users can now select the new option **Collect Android bug report** to include bug report in the device logs. **Note**: Requires MaaS360 for Android agent 7.10 or later. Supported only on Android Enterprise devices that are enrolled in Device Owner (DO) mode. The process of bug report collection takes up to 10 minutes.

Android 7.05 release summary

MaaS360 makes the Android app version 7.05 beta available in Play Store on 16 April 2020.

MaaS360 for Android core

Updated Device Enrollment Mode values in Device Summary for Android Enterprise devices >>

In the previous releases, MaaS360 displayed inaccurate values for Device Enrollment Mode attribute in the Device Summary page. For Android Enterprise use cases, the attribute **Enrollment Mode** displayed **Container Type status** on Device Summary page such 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.

MaaS360 rolls out the change to read the right values for **Enrollment Mode** for both deployment models Android Enterprise and Device Admin **-** as **QR Code**, **Google Zero Touch**, **Knox Mobile Enrollment, DPC Identifier** (for AFW#) or **Android Configurator** wherever such information is available and captured by the app.

MaaS360 also extends **Container Type** attribute for Device Admin devices which will read accurate values such as **Device Administrator**, **Samsung Device Administrator**, **Zebra Device Administrator**, **Bluebird Device Administrator**, etc, wherever OEM custom SDK has been integrated.

Note:

- MaaS360 has programmatically migrated **all device groups** and **home page watch lists** using **Device Enrollment Mode** attribute (to track and group Device Owner and Profile Owner devices) to use **Container Type** attribute. The policy/rule assignments and application/document distributions will remain intact with this migration.
- 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 app 7.05+.
- For devices running MaaS360 for Android versions below 7.05, and where administrators have not re-generated QR code or ZT JSON profiles, the enrollment mode isn't captured by the app already; as a result, the device summary and smart search will show **Device Enrollment Mode** attribute value as **Not Available.**

Defect Fixes

Defect Number	Summary
39473	The QR code based Android Enterprise Device Owner enrollments failed.
39426	The token based Android Enterprise Device Owner enrollments failed.
39160, 38871	After a restart, kiosk launcher crashed when attempting to enter Kiosk mode.

Android 7.0 Release Summary

MaaS360 makes the Android app version 7.0 beta available in Play Store on 16 March 2020.

Location permission requirements on Android 10+ devices >>

With the new permission changes in Android 10, users are required to turn on location service and grant location permission to MaaS360 app so the app can display configured SSID in Corporate Settings in MaaS360 agent and report last connected SSID to portal.

MaaS360 Kiosk app requires location permission to display configured Wi-Fi networks and Bluetooth devices in close range. The devices cannot discover Wi-Fi networks and Bluetooth devices until the location service is turned on.

Note: If the permission is blocked due to policy, the user will not be able to turn on the location service on the device.

New languages support for MaaS360 agent >>

MaaS360 agent is now available in three new languages: Hungarian, Danish and Turkish.

Note: Supported only for MaaS360 Core app. The feature is not applicable to MaaS360 Secure Container (first-party) apps.

Enforce device lock-down on devices that escape Device Owner enrollment >>

To discourage skipping of Device Owner enrollment, MaaS360 restricts important features on the device until the device is completely enrolled. When users skip Device Owner enrollment at any stage after MaaS360 app is installed (or activated) as Device Owner, MaaS360 enforces following restrictions on the device:

- Account management: Users cannot access Play Store, add, or delete personal accounts such as GMail.
- App management: Users cannot uninstall or install apps from Play Store and or from other sources such as Android Debug Bridge (ADB).

Notification badge support for MaaS360 Secure Container apps >>

In the previous releases, MaaS360 added notification badge support for all third-party apps in Kiosk launcher. In this release, MaaS360 extends the notification badge support to MaaS360 Secure Container apps in Kiosk mode. Users can turn the badge notifications on/off through Kiosk settings.

Reduce the size of inline and attached images in Secure Mail >>

MaaS360 adds support to limit the size of the inline images and picture attachments that are uploaded to Secure Mail. When users upload a picture that exceeds the maximum inline or attachment limit, MaaS360 displays options (Original, Small, or Medium) that allow them to reduce the size.

Note: When the image size is scaled down, the resolution is also reduced when the image arrives at the destination.

Open/share third-party app data using Secure Editor and Docs >>

In the previous releases, MaaS360 restricted the use of Secure Container apps to access corporate content. In this release, MaaS360 removes the restriction to allow files from third-party apps to be opened and shared with Secure Viewer/Editor and MaaS360 Docs respectively. MaaS360 Viewer/Editor and Docs app work as shared resources in an Android Enterprise enrolled device. For example, users can now edit a Word document in the Files app with Secure Editor and then Share it to Docs app. When a supported file type is opened, Secure Editor/Secure Viewer is shown in **Open with** menu and MaaS360 Docs is shown in **Share via** menu.

Note: Applicable to Android Enterprise devices. Requires MaaS360 for Android 7.0. In Profile Owner mode, the files in Personal profile cannot be opened/shared with with Secure Container apps.

Flexible in-app updates for MaaS360 Secure Container apps >>

MaaS360 adds support for flexible in-app updates, allowing users to update MaaS360 Container apps to Play Store version directly from within the app without even going to Play Store app.

Defect Fixes

Defect	Summary
39145	Fixed: MaaS360 launcher crashed on DO enrolled device in Kiosk mode when custom status bar is enabled.

38860, 38689	Fixed: The wi-fi proxy settings pushed via policy are not configured on Android Enterprise devices enrolled in Device Owner mode.
38834	Fixed: Unflagged emails in MaaS360 Secure Mail app are not synced to Microsoft Outlook.
38801	Fixed: The signed messages cannot be forwarded if the signing certificate is unavailable in Secure Mail.
38738, 38620	Fixed: The devices are incorrectly classified as Smartphone instead of Tablet.
38680	Fixed: The .txt files could not be opened with MaaS360 Secure Viewer in Android 10 devices.
38475	Fixed: The Word docs in MaaS360 Docs app could not be opened with Secure Viewer app.
38412	Fixed: MaaS360 Secure Editor shows inaccurate values for Excel calculations.
38332	Fixed: Files could not be opened with MaaS360 Secure Viewer after re-enabling permissions.
37670	Fixed: Unable to send pictures with high resolution through MaaS360 Secure Mail app.
37536	Fixed: Yellow exclamation mark is displayed in Secure Container, background sync is stopped, and the user is prompted to re-input their password manually.
37535	Fixed: Corporate Wi-Fi is disconnected even though the domain password is updated in MaaS360 app.
37512	Fixed: PO device enrollment stuck in "Reset Password Token" screen

Android 6.95 Release Summary

MaaS360 makes the Android app version 6.95 available in Play Store on 17 February 2020.

MaaS360 for Android core

Report suspicious emails to administrators >>

MaaS360 now allows MaaS360 Email users to report suspicious emails to their administrators. When an email is reported as spam, administrators receive an email notification and the email is deleted from the mailbox. Administrators can use the Persona policies to configure report phishing settings.

Validation for Bluebird firmware updates

When pushing Bluebird OS update through MaaS360 Push Profile action, MaaS360 performs a validation check on the eMMC size of the Bluebird device before performing OS upgrades on the selected models (EF500 and EF400). The validation is performed on the following partitions:

- '/sys/block/mmcblk0/size'
- '/sys/block/mmcblk0/mmcblk0p33/size'

If the validation is unsuccessful, the OS upgrade will fail with an error message that is displayed in the Action History for the device.

Improvements to Always-ON F5 VPN connections

- When Always On is enforced on Android Enterprise devices, MaaS360 now allows the newly installed (whitelisted) apps to use the VPN connection automatically. In the previous releases, users had to reboot the device or reconnect VPN setting manually.
- When any configuration settings are changed by the administrator within policy, the configuration is automatically applied to the device without interrupting the VPN connection. In previous releases, VPN was disconnected and users had to manually apply the new configuration from MaaS360 Corporate Settings.

Deprecation of LG OEM API support for Device Admin on Android 9 + devices

Effective Android 9, MaaS360 deprecates OEM API support for LG devices that are enrolled in Device Administrator mode. Customers using LG specific policies are recommended to migrate to Android Enterprise and use LG OEMConfig app for OEM policy support.

With this deprecation,

- On existing devices that upgrade to Android 10, the OEM specific apps **MaaS360 for LG** will be removed.
- New Android 9 + devices enrolled as device admin will not receive the OEM app **MaaS360 for LG** during device enrollment. The devices will be enrolled as regular Android devices.
- MaaS360 will not support LG specific APIs on these devices. As a result, LG specific policies will not apply on Android 9 Device Admin devices.
- For app installations, "Install Automatically" option will not be supported on these devices.

Support for biometric authentication on Work Profile >>

MaaS360 adds support for biometric identity for Work Profile access on devices that offer such support on Work Profile. Users will be guided with stepwise instructions to enable biometrics based on the device manufacturer and OS version, under MaaS360 Settings > Passcode > Enable Biometrics.

Defect Fixes

Defect number	Description
38525	Fixed an issue wherein the devices failed to relaunch into Kiosk mode when the "Usage policy management" property was turned off.

Android 6.96 Release Summary

MaaS360 made the Android app version 6.96 available in Play Store on 19 February 2020.

Defect number	Description
38929	Fixed intermittent Android Enterprise DO mode enrollment failures.

iOS Release Summaries

Release information for MaaS360 iOS Applications

Secure Browser 3.31.7 Release Summary

MaaS360 makes the iOS Secure Browser app version 3.31.7 available on iTunes on 22 December 2020.

- Added minor bug fixes.

iOS SDK 3.30.955 Release Summary

MaaS360 makes the iOS App Wrapping version 3.30.955 available on 15 December 2020.

Defect	Summary
41565	The URL in the wrapped app was truncated when opened in Secure Browser.

iOS 4.0 Release Summary

MaaS360 makes the iOS app version 4.0 available on Test Flight on 30 November 2020.

Apple WKWebView implementation in MaaS360 for iOS app >>

MaaS360 replaced UIWebView component with WKWebView for enhanced HTML rendering performance, smooth scrolling, security and reliability in application workflows.

Multitasking support for MaaS360 for iOS app >>

MaaS360 adds support for split-view multitasking for iPads, allowing users to use MaaS360 for iOS app alongside other iOS apps. For example, you can view the Secure Mail app and Apple Notes (or any other Native app) side-by-side at the same time. In the first phase of series of enhancements, MaaS360 introduces multitasking support for Email, Calendar, etc, and adapts different multitasking modes: compact, regular, and Slide Over. **Note**: Requires MaaS360 for iOS app version 4.0 or later. Multitasking support will be extended to iOS Secure Editor and Secure Browser in the future releases.

Block remote images for external domain emails >>

MaaS360 adds support to block remote URL referenced embedded images in emails that are received from external domains. MaaS360 prevents the auto-download of remote images in mail content when the emails are opened in the Secure Mail app. This feature is applicable to primary, secondary, and delegation accounts. Administrators can use new security policies to define which emails can be classified as external emails. For more information, see https://www.ibm.com/support/knowledgecenter/en/SS8H2S/com.ibm.mc.doc/pag_source/concepts/persona_policy_gde_mail_security_stng.htm

Deprecation of support for iOS 11 devices >>

MaaS360 for iOS app version 4.0 will not be supported on iOS 11 devices.

Support to skip the strict user account validation >>

Administrators can now skip the strict user account validation if the Office365 accounts are inaccurately flagged as restricted in the Secure Mail app. Follow these steps to skip the strict user account validation:

1. Navigate to **Security** > **Policies** and then open a Persona policy.
2. Navigate to **WorkPlace** > **Security** > **Configure Other Settings** > **Advanced Configuration Details**
3. Add the following key/value pair.

    - Key: **Office365SkipUserParamsValidation**.
    - Value: **true**

Defect Fixes

Defect	Summary
41550	Apple Watch users could not set a PIN when Touch ID is off.
41233	The corporate support information provided in the MaaS360 portal was not synced to the already enrolled iOS devices.
40778	When users try to print a document, the document was successfully printed despite showing the Request Declined error message.
39607	Password prompts were displayed for the customers that enabled certificate-based authentication. Fix: 1. Open Persona policy 2. Navigate to WorkPlace > Security > Configure Other Settings > Advanced Configuration Details and then provide the following key-value pairs: Primary account: • Key: DisablePrimaryMailboxPasswordWithCert • Value: Yes Secondary account: • Key: DisableSecondaryMailboxPasswordWithCert • Value: Yes
39139	MaaS360 for iOS app crashed when other apps were in use and the MaaS360 app was running in the background.
38609	The forwarded attachment for the Report Phishing feature was missing original headers.

Defect	Summary
33135	Customers could export content to apps outside of MaaS360 secure container when using the iOS Multitasking feature.
29553	The images in the email were distorted before the MaaS360 app upgraded to WKWebView from UIWebView.

iOS Secure Editor 2.70.102 Release Summary

MaaS360 makes iOS Secure Editor app version 2.70.102 available on Test Flight on 15 December 2020.

- Added minor security improvements.

iOS Secure Browser 3.30 and iOS 3.400 Release Summary

MaaS360 makes the iOS Secure Browser app version 3.30 available for Beta testing on 16 November 2020.

MaaS360 makes the MaaS360 app for iOS version 3.400 available for Beta testing on 16 November 2020.

Both releases include the following defect fixes:

Defect Fixes

Defect	Summary
41406	When users try to log into the MaaS360 app, the app hangs at the Configuring screen.
40969	When a device is assigned a user after enrolling in DEP without a user, the persona policies are stuck in pending state without reaching the device.
13077	Fixes for the direct mode in Enterprise Gateway supporting Apple's WKWebView

iOS SDK 3.30.960 Release Summary

MaaS360 makes the iOS SDK version 3.30.960 available on 30 October 2020.

All the UIWebView references have been removed from the MaaS360 SDK framework and its dependent libraries.

iOS SDK 3.30.950 Release Summary

MaaS360 makes the iOS SDK version 3.30.950 available on 16 October 2020.

Defect Fixes

Defect Number	Description
40598	An app wrapped with iOS SDK crashed when the users tap the viewWillAppear controller after opening the app.

iOS Secure Browser 3.21 Release Summary

MaaS360 makes the Secure Browser app version 3.21 available in App Store on 28 September 2020.

iOS 14 Zero-day support

MaaS360 continues to support all the Secure Browser features and fixes minor issues to provide seamless browsing experience on iOS 14 devices.

Support for new Import to MaaS360 share action menu >>

MaaS360 adds a new action "**Import to MaaS360"** to the System share action menu to allow users to easily share a list of files with MaaS360 application to either save to Docs or share with others over mail. The **Import to MaaS360** action replaces the **Copy to MaaS360** option that was shown in previous OS versions.

MaaS360 stops clipboard use for passcode management >>

With the new privacy update for clipboard data security, Apple added a new banner alert to iOS14 that notifies users when an app reads the contents of a clipboard. MaaS360 proactively reads the clipboard data to protect corporate data copied to it and to enforce container passcode policies specified by the administrator among the container apps. With MaaS360 for iOS version 3.200, MaaS360 stops clipboard use for passcode management to avoid the banner alerts on iOS 14 devices except for the scenarios wherein the end-user explicitly performs a paste operation. **Note**: This change impacts only customers that have **Disable Keychain Check** enabled.

Behavior changes

When Browser switches from MEG 3.0 to 2.0, a VPN Configuration Update message is displayed and the Browser switches to the MaaS360 for iOS app to apply the configuration.

Defect Fixes

iOS Secure Editor 2.70 Release Summary

MaaS360 makes the iOS Secure Editor app version 2.70 available on Test Flight on 16 September 2020.

MSAL integration for Secure Editor >>

MaaS360 extends Microsoft Authentication Library (MSAL) framework support to Secure Editor. Effective 2.70, Secure Editor upgrades to new Microsoft identity platform endpoint Microsoft Authentication Library (MSAL) version 1.1.5 from Azure Active Directory Authentication Library (ADAL) for more secure and better single sign-on experience with Office365 Mail, SharePoint, OneDrive services.

WKWebView support

MaaS360 deprecates UIWebView in favor of WKWebView class for the Secure Editor app. WKWebView offers a lot of benefits over UIWebView such as smooth scrolling, improved rendering performance, and so on.

Defect Fixes

Defect #	Summary
35986	iOS Secure Editor users could not use the Microsoft Authenticator app for multi-factor authentication to edit OneDrive and SharePoint docs.

iOS 3.200 Release Summary

MaaS360 makes the MaaS360 app for iOS version 3.200 available on iTunes on 28 September 2020.

MaaS360 stops clipboard use for passcode management >>

With the new privacy update for clipboard data security, Apple added a new banner alert to iOS14 that notifies users when an app reads the contents of a clipboard. MaaS360 proactively reads the clipboard data to protect corporate data copied to it and to enforce container passcode policies specified by the administrator among the container apps. With MaaS360 for iOS version 3.200, MaaS360 stops clipboard use for passcode management to avoid the banner alerts on iOS 14 devices except for the scenarios wherein the end-user explicitly performs a paste operation. **Note**: This change impacts only customers that have **Disable Keychain Check** enabled.

Behavior change when precise location permission is not granted >>

iOS 14 gives users the choice to grant either approximate or precise location permission to an application on the device. Precise location permission to MaaS360 application helps in getting the exact coordinates of the device location otherwise it can determine the approximate location. This new change can impact some important Admin configured location-based features such as location tracking and region monitoring.

Support for new Import to MaaS360 share action menu >>

MaaS360 adds a new action "**Import to MaaS360"** to System share action menu to allow users to easily share a list of files with MaaS360 application to either save to Docs or share with others over mail. The **Import to MaaS360** action replaces the **Copy to MaaS360** option that was shown in previous OS versions.

Renamed PIN to Passcode across all iOS agent screens >>

To provide a consistent user experience on iOS and Android agents, MaaS360 renames the container lock **"PIN"** to **"Passcode"** across all iOS agent screens. With iOS agent version 3.200, all references to PIN such as labels, warning messages, headings, and so on will now be changed to Passcode.

Defect fixes

Defect	Summary
40688	MaaS360 app crashed when users tried to access the Secure Mail app or Calendar app.
40420	MaaS360 reported incorrect mobile data usage.
41209	Users were able to print PDF documents from the MaaS360 Secure Container even though printing capabilities were disabled through policies.

Known issues

- The native mail attachment items cannot be imported via Import to MaaS360 share action menu.
- When users try to open a file with an application that does not support the Share extension such as Microsoft Office, Boxer, MaaS360 Editor, Excel, etc, the file is opened on the app, but when users return to the Share sheet, the other apps on the Share sheet become unresponsive.

iOS Browser 3.20.500 Release Summary

MaaS360 makes the iOS Secure Browser app version 3.20.500 available on iTunes on 18 August 2020.

Defect Fixes

Defect	Summary
40810	The URLs were inaccessible in Secure Browser on devices running iOS 14.
40813, 40890, 40801	A blank white screen was displayed on web pages after Secure Browser upgraded to the latest version.

iOS Browser 3.20 Release Summary

MaaS360 makes the iOS Secure Browser app version 3.20 available on iTunes on 31 July 2020.

Support for Apple UIWebView Deprecation

Details found here

Defect Fixes

Defect	Summary
40278	The error message **Cannot verify server identity** was displayed when accessing the intranet sites. To avoid the prompt, customers must use the following key-value pair in the advanced configuration policy: • Key: **secureBrowserAcceptBadCertURLs** • Value: <www.expired.badssl.com>

PIV-D 1.35.5 Release Summary

MaaS360 makes the PIV-D app version 1.35.5 available in iTunes on July 20, 2020.

- Entrust SDK is upgraded to version 3.6.0**.**

Defect fixes

Defect Summary 39981 The Exchange ActiveSync policy settings were not configured on the device when the authentication was set to MaaS360 Derived Credentials.

iOS 3.99.500 Release Summary

MaaS360 makes the iOS app version 3.99.500 beta available on iTunes on 09 July 2020.

ADAL to MSAL migration >>

With MaaS360 core app version 3.99.500, MaaS360 upgrades to new Microsoft identity platform endpoint Microsoft Authentication Library (MSAL) version 1.1.5 from Azure Active Directory Authentication Library (ADAL) for more secure and better single sign-on experience with Office365 Mail, SharePoint, OneDrive services.

Support for Apple UIWebView Deprecation

Details found here

Defect fixes

Defect	Summary
40297	The installation of the Secure Browser app through MaaS360 app failed with an error message.
40404	MaaS360 app does not prompt for a PIN/Passcode after the app timeout.
40659	iOS DEP shared devices could not authenticate to the MaaS360 app.
40464	When a user approves a password reset request through Secure Mail app, a hyperlink was automatically created in the email response that was sent to the administrator. **Note**: After the fix, the hyperlink will not be displayed in the Compose email screen, but it will be displayed in Outbox and Draft folders similar to the native email client.
40313	The certificate download requests were displayed even though the required certificates were downloaded.

iOS Browser 3.10.25 Release Summary

MaaS360 makes the iOS Secure Browser app version 3.10.25 available on iTunes on 07 July 2020.

- MaaS360 adds MEG 3.0 support.

Defect fixes

Defect #	Description
40126, 40124, 40083, 40034	External links in Secure Mail such as Microsoft Forms could not be opened in Secure Browser. When the links to external sites were opened, Secure Browser displayed **Bad Request – Invalid URL** error message.
40059	The links on a website that uses UIWebView were opened in a new Window instead of opening in a different frame in the same Window.
38411	The inputs provided via custom on-screen keyboard were delayed in Secure Browser.

iOS SDK 3.30.900 Release Summary

MaaS360 makes the iOS SDK version 3.30.900 available on 15 May 2020.

Defect Fixes

Defect Number	Description
39740	Face ID / Touch ID authentication was disabled and enterprise apps fall back to PIN for authentication after upgrading to latest SDK.
38245	The enterprise iOS apps wrapped with MaaS360 could not connect to MaaS360 SDK Gateway during the MaaS360 portal maintenance window.

iOS 3.99 Release Summary

MaaS360 will make the iOS app version 3.99 beta available on iTunes on 08 June 2020.

Defect fixes

<table>
<tr><th>Defect</th><th>Summary</th></tr>
<tr><td>39971</td><td>MaaS360 app crashed when .MSG file was opened via AVA app.</td></tr>
<tr><td>38931</td><td>The PIN screen was not aligned to center and overlaps status bar on MaaS360 Watch app</td></tr>
<tr><td>38568</td><td>Shared calendars were not displayed despite giving right permissions.</td></tr>
<tr><td>38411</td><td>The custom on-screen keyboard inputs were delayed in Secure Browser.</td></tr>
<tr><td>38378</td><td>Duplicate attachments were displayed in Secure Mail when forwarding email.</td></tr>
<tr><td>38129</td><td>The deleted emails re-synced to device in Secure Mail.</td></tr>
<tr><td>37382</td><td>When adding a delegate mail account, the sync failed despite giving right permissions.</td></tr>
<tr><td>40061</td><td>The Zoom meeting info is truncated; as a result, users could not dial in automatically.</td></tr>
<tr><td>39652</td><td>

The Microsoft Teams meeting ID was not displayed after dial in.
When users dial in to the meeting by clicking the invitation, the conference id was automatically dialed after the phone number, but users could not join the meeting.
To get the Join button for different conferencing tools, administrators must add the corresponding value in the advanced configuration against the key calOtherMeetingURLHosts. The value is part of base URL of the event.

Path: Persona policy > WorkPlace > Security > Advanced Configuration Details

Examples:
<table>
<tr><th>URL</th><th>Value</th><th>Key</th></tr>
<tr><td>https://zoom.us
/j/9583234444?pwd=b324dKmwUnlJz09</td><td>zoom.us</td><td rowspan="4">calOtherMeetingURLHosts</td></tr>
<tr><td>https://f5networks.zoom.us

/j/9543378844?pwd=h67nDki07Yt</td><td>f5networks.zoom.us</td></tr>
<tr><td>https://paloaltonetworks.zoom.us

/j/9543378844?pwd=h67nDki07Yt</td><td>paloaltonetworks.zoom.us</td></tr>
<tr><td>https://teams.microsoft.com/l/meetup-join/19%3ameeting_YUGTSFDTyDbNSSSYWET/0?context=%7b%7ddg-y66d></td><td>teams.microsoft.com/l/meetup-join</td></tr>
</table>
</td></tr>
</table>

iOS Browser 3.00.153 Release Summary

MaaS360 makes the iOS Secure Browser app version 3.00.153 beta available on iTunes on 23 April 2020.

Defect Fixes

Defect Number	Description
38746	The files with XDW extension could not be downloaded via Secure Browser. With this fix, when XDW files are opened, MaaS360 now directly downloads the XDW files, just like .zip files, without displaying a preview.
38741	A grey page is displayed when PDF files are opened instead of loading a preview.
38345	The PDF files are truncated without allowing users to scroll through the files.

iOS 3.98.95 Release Summary

MaaS360 makes the iOS app version 3.98.95 available on App Store on 13 April 2020.

Defect Fixes

Defect Number	Description
39488, 39436	Activation of customer SDK apps failed on iOS 13 and later devices. **Note**: MaaS360 does not support activation of SDK apps version 3.30.500 or lower.

iOS 3.98 Release Summary

MaaS360 makes the iOS app version 3.98 beta available in iTunes on 3 March 2020.

MaaS360 for iOS (core app) Enhancements

`WKWebView` support for MaaS360 mail compose screen >>

MaaS360 deprecates UIWebView in favor of WKWebView and uses the latest WKWebView class for email compose screen. With this replacement, the dictation support is added back to the compose email screen.

This feature is supported on following devices:

- iPad (iOS 13), iPhone (iOS 12+)

End of support for devices running iOS 10 or lower >>

To provide optimum security and performance, MaaS360 announces the end of support for iOS devices running 10 or lower. After iOS 3.98 release, MaaS360 stops support for any bug fixes pertaining to iOS version 10 or lower.

Known issues

Effective 3.98, with the Apple's new privacy restrictions:

- When **Restrict Import of Files** persona policy is enabled on iOS 13 and later devices, none of the apps (including the first-party apps) are allowed to share files to MaaS360 app. However, users can share files to the MaaS360 app from Secure Browser, Secure Editor, and SDK/Wrapped apps on iOS 12 or lower versions.
- MaaS360 does not support activation of SDK apps version 3.30.500 or lower.

Defect Fixes

Defect number	Description
38492, 38161	Matching suggestions are not displayed in auto-complete list when composing emails in Secure Mail.
38463	When a Microsoft Teams meeting invite is opened, Secure Mail failed to launch the Microsoft Teams app.
38453	Secure Mail app crashed when images are shared from iPad via Share Extension.
38112	Large files that are sent via Secure Mail are inaccessible in Outlook.
37868	Before upgrading to WKWebView, Secure Mail crashed while replying/forwarding emails.
37751	Face ID could not be enabled after password reset.
37552	When replying to an email in Secure Mail, the email history is not displayed on selecting **Load whole message** option.
37407	Before upgrading to WKWebView, the use of Keyboard dictation was disabled in Compose email screen.
36083	The Secure Mail app froze if Inbox contains mails with a large number of conversation threads.
38800	The French localization for the string **Report Phishing** in Secure Mail is incorrect.

PIV-D 1.30.115 Release Summary

MaaS360 makes the PIV-D app version 1.30.115 available in iTunes on January 14, 2020.

MaaS360 PIV-D enhancements >>

- MaaS360 reads the **NT Principal Name** value from the PIV Authentication certificate and displays the value in the **Authentication Certificate** > **Subject Alternative Name** field.
- MaaS360 makes signing and encryption certificates optional for MaaS360 PIV-D app configuration and displays an alert message if those certificates are unavailable. However, users will still be able to configure and use the MaaS360 PIV-D app without interruption. In the previous releases, the authentication, signing, and encryption certificates were mandatory and users were restricted from using the app if one of those certificates was unavailable.

iOS Browser 3.0 Release Summary

MaaS360 will make the iOS Secure Browser app version 3.0 beta available on iTunes on 20 May 2020.

WkWebView support >>

Effective 3.0, MaaS360 upgrades to `WKWebView` class from `UIWebView` to embed web content in Secure Browser app. WKWebView offers a lot of benefits over UIWebView such as smooth scrolling, interactive web content, improved rendering performance, and so on. However, users can also switch to `UIWebView` anytime they want.

Note:

- Requires iOS 11 and later.
- MaaS360 will extend `WKWebView` support to MaaS360 Enterprise Gateway customers with MEG 3.0 beta, which will be released in April. MEG 2.0 customers must switch to `UIWebView` to access intranet sites until MEG 3.0 is released.
- The changes are applied to Secure Browser on relaunch of the app.
- `UIWebView` will be default webview for the customers using MEG 2.0.

Switching to UIWebView

Non-Gateway customers facing issues with `WKWebView` can use the following advanced configuration flag to switch to old `UIWebView`

1. Navigate to Persona policy > WorkPlace > Security > Advanced Configuration Details and then provide the following key and value:

   - Advanced Configuration Flag Name : **secureBrowserUIWebViewEnabled**
   - Value of the flag : Yes/No (Yes - UI & No - Wk)

After switching, the Configuration Change message is displayed in Secure Browser to ensure that the configuration is applied.

Behavior changes in WKWebView

- The Settings > Accept Cookies > From Visited option is disabled.
- Custom headers are not supported.
- Opening of multiple windows is supported.
- If a website enforces downloading of a file using "content-disposition: attachment; filename" header in the response, Secure Browser automatically downloads such files and displays in quicklook controller.

Defect Fixes

Defect number	Description
37854	Secure Browser app did not display **Images in Gallery** menu in Microsoft Outlook Web App (OWA).
38953	The text inputs are not updated in Secure Browser.
38276	The print preview for PDF file with landscape orientation is shown in portrait orientation.
37756, 37645, 37629, 37439, 36806, 36786, 36687, 37731, 34016, 32996	MaaS360 upgrades to `WKWebView` class from `UIWebView` in Secure Browser to: • Improve the rendering performance • Accurately run JavaScript objects • Access folders in Microsoft OneDrive site without fail • Render images, videos, links, Microsoft Forms, and Office 365 sites correctly

Cloud Extender Release Summaries

Release information for Cloud Extender

Cloud Extender 2.103.x Release Summary

The following new features were introduced in this release:

- Certificate Integration module support for the Cisco EST certificate enrollment protocol

  The Certificate Integration module now supports the Cisco EST (Enrollment over Secure Transport) certificate enrollment protocol. For more information about how to configure the Cisco EST certificate template that integrates with Cloud Extender, see https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/ce_source/concepts/ce_ca_est.htm.

- Email Notification module support for Modern Authentication for Office 365 integration

  The Email Notification module now supports Modern Authentication for Office 365 integration in response to the announcement that Microsoft started to disable support for Basic Authentication in Exchange Online that began in October 2020. For more information about this announcement, see https://developer.microsoft.com/en-us/office/blogs/deferred-end-of-support-date-for-basic-authentication-in-exchange-online/.

  For Modern Authentication support, the new Cloud Extender Configuration Tool provides an option to choose the preferred authentication method as Basic Authentication or Modern Authentication.

  If you select Modern Authentication, you must enter the Tenant ID and the Client ID that you create in the Office 365 Admin Portal. The procedure on how to create the Tenant ID and the Client ID in the Office 365 Portal is documented in step 5 at https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/ce_source/tasks/ce_exchange_int_notifications_config.htm.

CVE Security Bulletins

The following CVE security bulletins were issued for this release:

- MEG: https://www.ibm.com/support/pages/node/6403860
- Cloud Extender agent: https://www.ibm.com/support/pages/node/6403864

To Upgrade Cloud Extender Agent and MEG Modules

- MEG: IBM Documentation Page
- Cloud Extender agent v2.103.000.51 : IBM Documentation Page

Cloud Extender 2.102.x Release Summary

The following new feature was introduced in this release:

- **Exchange ActiveSync module support for Modern Authentication for Office 365 integration**
  The Exchange ActiveSync module now supports Modern Authentication for Office 365 integration in response to the announcement that Microsoft is starting to disable support for Basic Authentication in Exchange Online beginning October 2020. For more information about this announcement, see https://developer.microsoft.com/en-us/office/blogs/deferred-end-of-support-date-for-basic-authentication-in-exchange-online/.
  For Modern Authentication support, the modern Cloud Extender Config Tool now provides a link to Microsoft that explains how to transition to Modern Authentication, and automatically checks whether the administrator has installed the required PowerShell V2 module. If the PowerShell V2 module is not installed, a reminder message notifies the administrator about the upcoming deprecation of Basic Authentication, and provides a link to instructions on how to transition to Modern Authentication.

CVE Security Bulletins

The following CVE security bulletins were issued for this release:

- Cloud Extender agent: https://www.ibm.com/support/pages/node/6403812
- Cloud Extender agent: https://www.ibm.com/support/pages/node/6403828
- Cloud Extender agent: https://www.ibm.com/support/pages/node/6403862

Cloud Extender 2.100.x Release Summary

The following new features were introduced in this release:

- The Cloud Extender installer package now implements two-factor validation, where the user enters an Account ID (same as the Billing ID) and the installer compares the input to the Billing ID that is embedded in the license key. If the Billing ID and the Account ID match, the installation continues. If the Billing ID and the Account ID do not match, a message box explains that the license key is not valid for the entered Account ID. For more information, see step 4 in the procedure at https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/ce_source/tasks/ce_install_sw.htm.

- The Cloud Extender uninstaller package now displays a warning message that all local MaaS360 services, records, and queued data will be removed from the Cloud Extender server when you uninstall Cloud Extender. For more information, see https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/ce_source/tasks/ce_install_sw.htm.

macOS Release Summaries

Release information for MaaS360 macOS Applications

macOS Agent 2.41.000 and Packager 1.43.100

MaaS360 makes macOS Agent 2.41.000 and Packager 1.43.100 available on November 20.

macOS agent enhancements

Deploy macOS updates to devices >>

MaaS360® allows you to remotely deploy the latest security patches and macOS updates to devices from the MaaS360 Portal.

Behavior changes with Apple macOS 11 Big Sur

Effective macOS Big Sur release, during the license-based enrollment, macOS agent will not auto-install the MDM profile after the download. The system will prompt the end-user to open and install the MDM profile from the System Preferences app. In the previous macOS versions, the profile was auto-installed without user intervention.

Packager changes

Minor change to support Big Sur macOS

Defect fixes

Defect	Summary
40577	The macOS DEP enrollments failed.

macOS 2.40.000.016 and App Packager 1.43.000.015 Release Summary

MaaS360 makes the macOS app version 2.40.000.016 and MaaS360 App Packager 1.43.000.015 available on January 27, 2020.

macOS app enhancements

- Minor fixes and improvements

MaaS360 App Packager enhancements

Parallel packaging, dark mode, and resumable notarization support for MaaS360 Packager >>

- **Parallel packaging:** Maa360 Packager now supports uploading multiple packages in parallel as opposed to uploading apps one at a time. In the previous releases, when a package was added, administrators had to wait until the upload is completed before uploading a new package.
- **Resumable notarization**: If MaaS360 Packager is terminated after an app is submitted for notarization, MaaS360 resumes notarization process from where it previously left off when the MaaS360 Packager is relaunched.
- **Dark mode**: MaaS360 adds dark mode support for MaaS360 Packager.

macOS App Catalog 1.53.000 Release Summary

MaaS360 makes the MaaS360 App Catalog version 1.53.000 beta available on March 31, 2020.

Defect Fixes

Fix number	Description
38194	MaaS360 fixes an issue wherein enterprise app updates pushed by admin did not appear in MaaS360 App Catalog on end user devices.

macOS App catalog 1.53.100.001 Release Summary

MaaS360 makes the MaaS360 App Catalog version 1.53.100.001 available on May 13, 2020.

Defect Fixes

Fix number
Description 39599 App catalog crash fix on macOS 10.13 or lower devices.