IBM Security MaaS360 with Watson

A deep dive into how MaaS360 supports any device and any operating system

IBM Security

IBM

The basics

This is your primer on IBM Security MaaS360 with Watson, IBM's industry-leading unified endpoint management (UEM) solution.

Before we dive in, let's make clear that, of course, any enrolled device can be locked to the passcode screen, pinged for its last known location, wiped remotely, have a passcode configured, have WiFi networks and VPN profiles distributed, and all of the other basic functions expected from bare bones mobile device management (MDM).

But in this era of instant connectivity, an increasingly mobile workforce, and the expansion of non-traditional wearable, ruggedized, and virtualized endpoints, we wanted to make sure you get a little bit more out of the content you download.

That said, if you're still curious what else IBM Security MaaS360 can do once you've finished thumbing through here, take it for a spin with a free trial or connect with an IBMer for a demo.

Contents

Apple Business Manager (ABM)

ABM is a consolidation of Apple's Device Enrollment Program (DEP) and Volume Purchase Program (VPP).

MaaS360 supports this shift and has a long history of securing and managing Apple devices, from iOS to macOS to the new iPadOS.

What can be accomplished with MaaS360 and Apple Business Manager?

Out-of-the-box enrollment
Apple devices come preconfigured for ABM with MaaS360 preinstalled. Administrators can automatically install software upon setup and limit end user configuration items.

Managed Apple IDs
Managed Apple IDs are company-owned IDs that employees can use to enroll a personal device in ABM via Apple's User Enrollment pathway.

Bulk app purchase and deployment
Purchase a number of app licenses from Apple to then distribute to employee devices as needed. As these are corporate-owned licenses, they can be revoked and redistributed upon an employee leaving or a device becoming unenrolled.

Advanced policy and compliance rules
From clearing activation lock to stringent app blacklists and whitelists, ABM extends management capabilities for corporate Apple devices.

Similarly to the larger topic of advanced policy and compliance, a device enrolled in Apple Business Manager (or Apple School Manager) can be "supervised," meaning admins can place additional restrictions such as blocking the use of Air Drop or access to the App Store.

Apple device policy highlights

iOS & iPadOS

From the simple to the complex, MaaS360 can satisfy any iOS and iPadOS use case through a comprehensive list of policy actions and restrictions.

App data migration restrictions
Restrict content from managed applications from being opened in unmanaged apps—and vice-versa.

Limiting backup options
Remove the ability to backup to iCloud or to a removable device.

Avoid device ownership headaches
Through ABM enrollment, ensure activation lock—the binding of an Apple ID to a device, making it near-impossible to reset to new if an employee has input their personal ID prior to departing the organization—does not brick a device.

Controlling app distributions
Single app mode through ABM enrollment can lock an iPhone or iPad to a single use kiosk can satisfy use cases from retail customers looking for self-service to medical professionals accessing health information on in-room tablets.

Strict app blacklisting and whitelisting through ABM enrollment serves specified use cases or simply guarantees corporate devices only run the apps the organization specifies.

Apple device policy highlights

macOS

macOS is an OS built to work in concert with other Apple devices, running many of the same apps found on the iPhone or iPad. This modern approach requires a modern UEM, and MaaS360 rises to the challenge. Beyond the backup limitations and app control outlined in the iOS and iPadOS section above, several key capabilities round out the robust macOS management features IBM offers, including:

Device encryption support

Configure FileVault 2 to encrypt macOS with XTS-AES-128 encryption.

- Create personal or institutional recovery keys
- Toggle whether a user must input the key after device hibernation
- Specify the number of times a user will be protmpted to enable FileVault before FileVault must be enabled for that user to successfully login

Keep users honest by only supporting trusted software

Enforce Gatekeeper settings to either allow the download of applications from anywhere or to limit downloads solely to the App Store and known developers.

Consistent system configuration

Is that system preferences pane a pain? Restrict the panes available to end users, dictating what can and cannot be adjusted on each macOS device.

Test OS version updates first

Delay automatic updates by up to 90 days, allowing IT & InfoSec to understand the potential risks associated with the newest macOS releases.

Device compliance & security highlights

Device compliance highlights
Take action when a user breaks with defined corporate policies. Is that iPhone jailbroken? Automated compliance rules can quickly remove corporate data or even fully wipe a device, taking immediate action upon detecting a compromised operating system.

What about something less severe? Maybe a personal Macbook is running an older version of macOS, leaving the device vulnerable. By setting a minimum operating system requirement, the user will be notified or even blocked from access to resources until they update their machine.

BYOD data loss prevention
Whether through the MaaS360 container or native data separation via User Enrollment, iOS comes equipped with controls to mitigate the unauthorized migration of corporate data.

With the MaaS360 container, the UEM app becomes a productivity suite, delivering mail, calendar, contacts, and other enterprise applications and resources to an encrypted sandbox built to restrict the copying, exporting, or even downloading of sensitive data without breaking the user experience.

All applications within this container or designed to mimic the look and feel of the native Apple mail, calendar, and contacts applications to make transitioning simple for all users.

iOS User Enrollment is a method introduced in iOS 13 allowing a device to split ownership between a personal Apple ID and a corporate Apple ID. This means that not only is data secured but user privacy is upheld by giving IT the ability to only view the corporate data.

While envisioned for BYOD usage, it isn't difficult to see its effectiveness for organizationally-owned devices as well as data accessed on the corporate side can be limited from interacting with the personal side of the device. Additionally, the corporate data can be easily removed as it creates a separate volume specific to those files.

Device compliance & security highlights

Mobile Threat Defense (MTD)
Beyond policy and compliance, additional risks still threaten the security of your users, devices, and data. Whether man-in-the-middle attacks preying on poorly configured home and public Wi-Fi or increasingly convincing phishing emails, users are constantly vulnerable to a growing landscape of threats. Via leading MTD vendor, Wandera, MaaS360 delivers proactive threat identification and remediation, whether that means taking action when a user connects to risky networks, blocking a browser from ever hitting a phishing landing page, or even detecting the telltale device slowdowns common to cryptojacking.

Identity and Access Management (IAM)
Deliver single sign-on (SSO) and multi-factor authentication (MFA) for cloud and enterprise apps via MaaS360 Identity, provided out-of-the-box through integration with IBM Cloud Identity. Used in conjunction with automated compliance rules, risk-based Conditional Access (CA) policies can be configured to ensure risky users are not interacting with sensitive data or other corporate resources.

Beyond this native workflow, MaaS360 and Identity can also be combined with an organization's existing SAML-based identity tools to again provide CA policies.

Native identity features available within MaaS360 and iOS, an organization's existing SAML-based identity tool can be integrated into the UEM deployment, either as the sole identity provider or in conjunction with the MaaS360 Identity feature to support conditional access.

TeamViewer remote support

At some point every user runs into an issue, whether something as simple as a forgotten passcode or a more complex connection or installation error. Ensure your users are well-supported from anywhere with TeamViewer and MaaS360. Through the MaaS360 console, launch TeamViewer and a remote session, either with the permission of the end user on an employee device or automatically for those endpoints unattended endpoints such as a kiosk or POS tablet.

Interested in learning more about what MaaS360 can do to support Apple deployments?

Start a trial

Android Enterprise enrollment

As an Android Enterprise Recommended solution, MaaS360 has been validated by Google as a platform capable of supporting advanced Android use cases.

While an Android device can be enrolled into MaaS360 through the legacy Device Admin (DA) manual enrollment method, this is not recommended as Google has made clear that critical Device Admin APIs are deprecated as of Android 10.

Android Enterprise enrollment methods

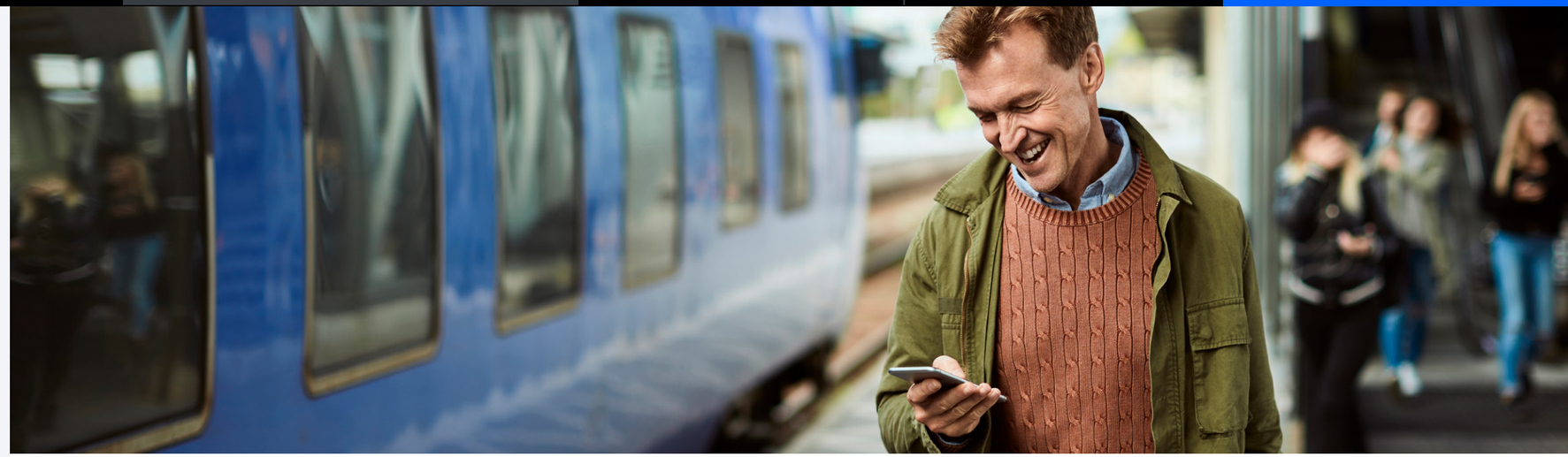
MaaS360 provides several native pathways to enroll into Android Enterprise.

Corporate-owned devices can be enrolled into fully managed Device Owner (DO) mode via any of the following options:

- Through a unique MaaS360 token
- Via a simple NFC bump
- Zero-touch provisioning (ZTP) for devices to be immediately configured upon factory reset or initial boot-up
- Through scanning of a unique QR code

Personally enabled devices, whether corporate or personally owned, can be enrolled in Profile Owner (PO) mode over-the-air (OTA) by allowing management access and inputting a managed Google Play account or authenticating a corporate Google account.

Samsung Knox Mobile Enrollment (KME)
For Samsung Knox devices, MaaS360 can apply Android Enterprise enrollment profiles directly through the KME portal, quickly bulk enrolling Samsung devices.



Android and Chrome OS device policy highlights

Android

Support for Android Enterprise Modes

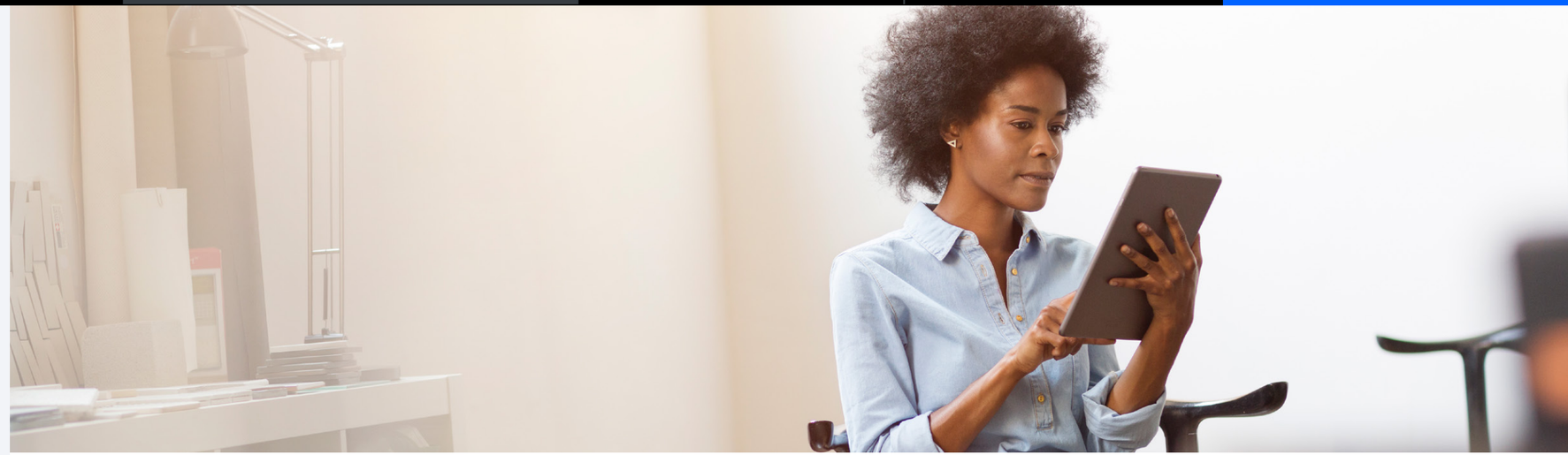
DO & PO

Through MaaS360, deliver Android Enterprise functionality for corporate and BYOD users. Distribute a manged Google Play store, take granular control of corporate devices—either through DO mode with a work profile or in a fully managed state—and support BYOD by distributing a work profile to personal device users in Profile Owner mode.

Specifically for BYOD Android devices previously enrolled in MaaS360 via DA mode, IBM provides a migration tool to seamlessly move those devices to PO mode without having to redo a lengthy re-enrollment.

Corporate-Owned, Single Use (COSU)

There are those specific use cases requiring a device to be locked down to a single app or group of apps. This is kiosk mode, and through MaaS360 and Android Enterprise, the highly secure COSU kiosk can be established. In this scenario, a device enrolled as COSU will disallow end user access to the features and Launcher settings than can, in some cases, “break out” of the kiosk. Additionally, this mode can be configured to not only provide a limited set of apps but instead automatically launch a single app and lock the screen to only display that interface.



Android and Chrome OS device policy highlights

Android

Support for Android Enterprise policy

Whether DO, PO, or COSU, MaaS360 and Android Enterprise can deliver custom policy configurations to support any use case with capabilities including:

- The ability to generate an applications blacklist and whitelist to limit what users are able to have installed on their devices
- Blocking the ability of end users to remove MaaS360 device management from their Android device
- Distributing VPN and Wi-Fi profiles during device setup so users are immediately connected and protected
- Silently installing or prompting the install of necessary applications as well as giving users the option to go the self-service route with a corporate Google Play or MaaS360 app store
- The option to immediately install, install during a specific maintenance window, postpone for 30 days, or freeze for 90 days any operating system updates
- Configuration of Access Point Name (APN) settings on Samsung devices
- Firewall rules to block traffic to and from a specific network location on any Android device

Android and Chrome OS device policy highlights

Chrome OS

MaaS360 can enroll and enforce policy settings on Chrome OS devices.

Device level APIs grant control over ONC files to establish network connections, ephemeral mode to ensure user data is not saved across sessions on shared devices, auto update settings, and many more.

User settings can configure blacklists and whitelists for Chrome and Android applications as well as specific URLs in the Chrome browser.

Kiosk mode allows for Chrome OS devices to be locked to specific applications, giving MaaS360 control over, not only the apps themselves but auto-launch launch controls, among other capabilities.

Device compliance & security highlights

BYOD and data loss prevention (DLP)
With the MaaS360 container, the UEM app becomes a productivity suite, delivering mail, calendar, contacts, and other enterprise applications and resources to an encrypted sandbox built to restrict the copying, exporting, or even downloading of sensitive data without breaking the user experience.

All applications within this container or designed to mimic the look and feel of the native Android mail, calendar, and contacts applications to make transitioning simple for all users.

Beyond the native MaaS360 container, Android Enterprise is renowned for its data separation capabilities. From PO mode establishing a separate work profile on the Android operating system devoted to the corporate applications a user needs to access on a personal device. These applications are denoted with a briefcase icon and can be configured to not share data with their personal counterparts.

DO mode can either distribute its own work profile for COPE deployments or fully manage the applications on the entire device, giving administrators control over any installed service or application to preserve DLP and give more granular control over the operating system.

Device compliance & security highlights

Mobile Threat Defense (MTD)

Beyond policy and compliance, additional risks still threaten the security of your users, devices, and data. Whether man-in-the-middle attacks preying on poorly configured home and public Wi-Fi or increasingly convincing phishing emails, users are constantly vulnerable to a growing landscape of threats. Via leading MTD vendor, Wandera, MaaS360 delivers proactive threat identification and remediation, whether that means taking action when a user connects to risky networks, blocking a browser from ever hitting a phishing landing page, or even detecting the telltale device slowdowns common to cryptojacking.

Identity and Access Management (IAM)

Deliver single sign-on (SSO) and multi-factor authentication (MFA) for cloud and enterprise apps via MaaS360 Identity, provided out-of-the-box through integration with IBM Cloud Identity. Used in conjunction with automated compliance rules, risk-based Conditional Access (CA) policies can be configured to ensure risky users are not interacting with sensitive data or other corporate resources.

Beyond this native workflow, MaaS360 and Identity can also be combined with an organization’s existing SAML-based identity tools to again provide CA policies.

TeamViewer remote support

At some point every user runs into an issue, whether something as simple as a forgotten passcode or a more complex connection or installation error. Ensure your users are well-supported from anywhere with TeamViewer and MaaS360. Through the MaaS360 console, launch TeamViewer and a remote session, either with the permission of the end user on an employee device or automatically for those endpoints unattended endpoints such as a kiosk or POS tablet.

Interested in learning more about what MaaS360 can do to support Android and Chrome OS deployments?

Start a trial

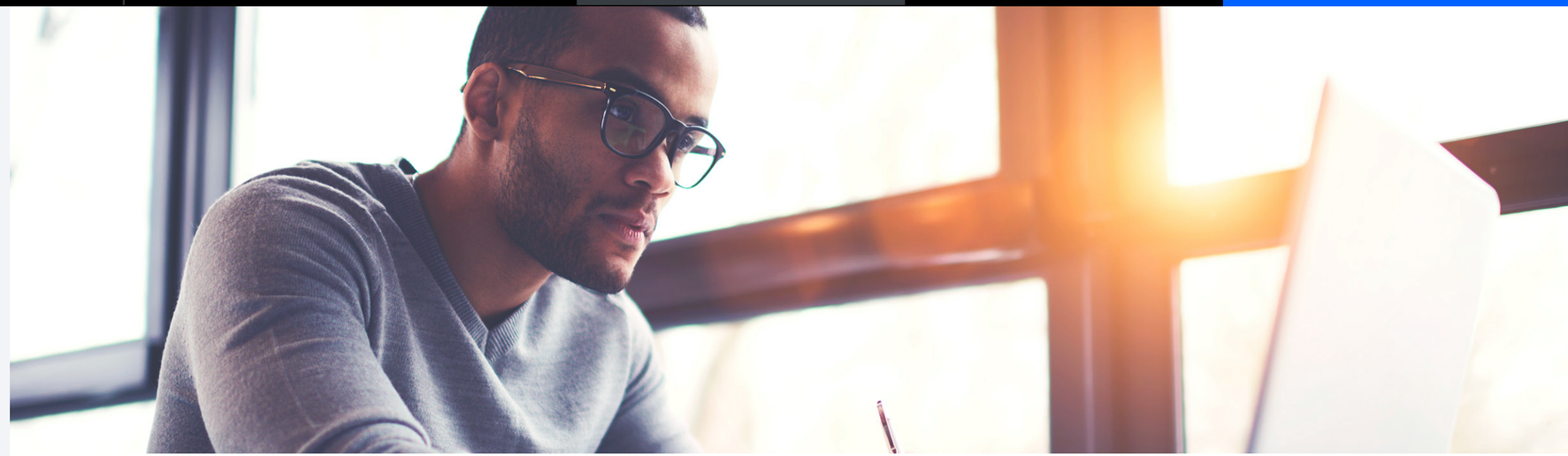
OOBE, Bulk Enrollment, Windows 10 Autopilot and Over-the-Air (OTA) enrollment

The Windows Out of Box Experience (OOBE) allows administrators to automatically enroll Windows 10 devices into MaaS360 when a user is registered with Azure Active Directory.

Windows Autopilot can also be configured to ensure that those devices enrolled via OOBE come preconfigured with the appropriate corporate settings, apps, and content.

Through the MaaS360 Windows 10 Bulk Provisioning tool, devices can be quickly enrolled via the traditional imaging method, or for those devices currently managed via client management tools (CMTs), migrated to MaaS360 via the Windows 10 Bulk Provisioning executable.

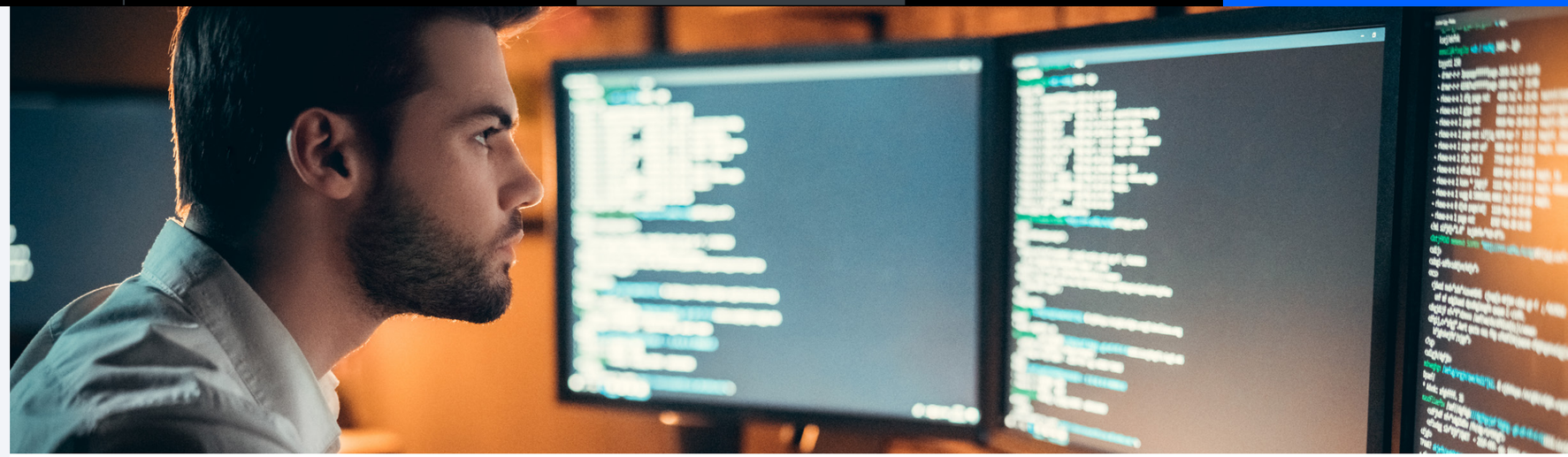
Administrator can also have team members enroll their devices by sending an over the air enrollment request to the user authenticating with a one time passcode or corporate AD credentials.



Supporting typical client management functions alongside Windows 10 Modern Management

Major analysts have coined “Modern Management” as a term defining the eventual shift towards managing and securing all devices in a single UEM console. To support this shift, MaaS360 includes a wide array of functions typically performed by a CMT:

- Distribute and install msi and exe applications, programs, scripts such as cmd, PowerShell, Python Scripts, and bat payloads to all Windows devices enrolled in MaaS360
- Actions similar to those available to Windows 10, macOS, and mobile operating systems, such as reboot, start/stop/restart service, lock, locate, and factory reset of device OTA
- Reports can be run to detect security software installed on devices to, for example, ensure antivirus is up-to-date and operational



Windows device policy highlights

Through extensive device policy settings, organizations can take granular control over their Windows 10 endpoints.

BitLocker
Enforce device encryption level through BitLocker and backing up recovery keys as needed

Windows Information Protection (WIP)
Determining which applications must be encrypted to protect corporate data via WIP

Windows Defender
Enabling and configuring scan settings for Windows Defender antivirus

Universal and desktop applications blacklists and whitelists
Limiting which apps should be installed on a given device or group of devices through Universal and desktop applications blacklists and whitelists

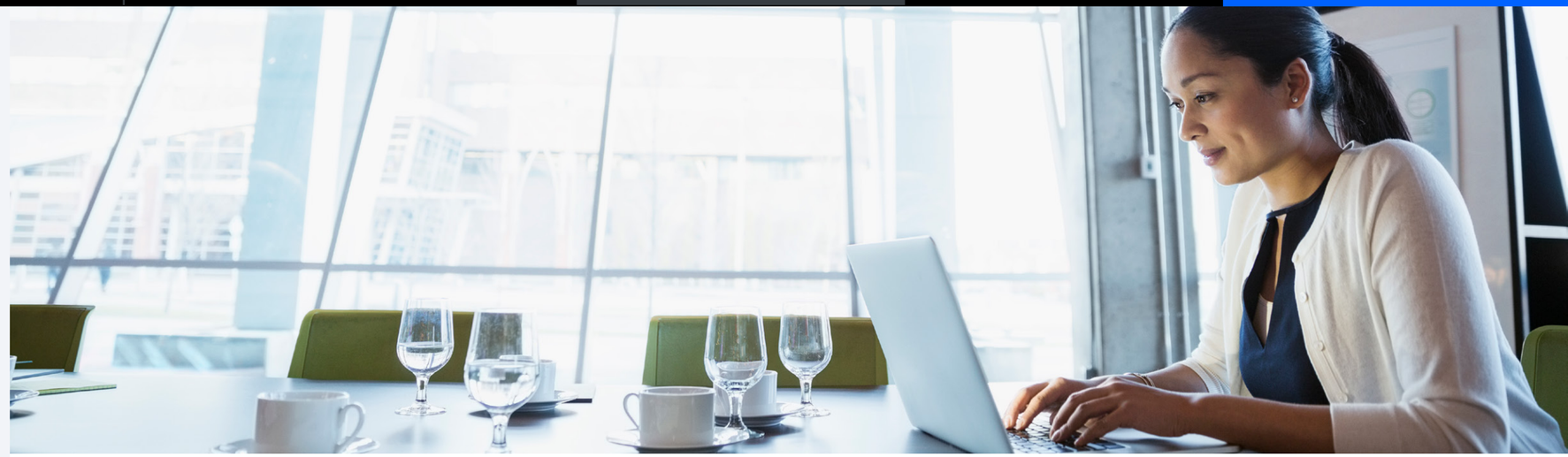
Windows device policy highlights

Through extensive device policy settings, organizations can take granular control over their Windows 10 endpoints.

Health Attestation
Configuring Health Attestation allows the health of a device to be assessed, from the code integrity to whether a device as booted in Safe Mode.

Windows Hello for Business
Activating Windows Hello for Business opens up the possibility of using a public key or certificate-based authentication to unlock a device.

Assigned Access
Assigned Access enables the configuration of a kiosk system with separate user accounts to not only secure shared devices but to lock those devices down to a single Universal app.



Patch, update, and support client management tool (CMT) co-existence and modern management

Take advantage of MaaS360's native patch and update management functionality for Windows 10, specifying the updates to apply to individual or groups of devices, the date and time for patch and update distribution, and generate reports on which devices have had patches successfully installed versus which are still missing critical updates. All this requires is an internet connection and an IP address, so it does not matter whether a device has a VPN is configured or is on the corporate network—or even in the office at all.

Delivery Optimization (DO)

For organizations looking to reduce the bandwidth issues that can come with traditional patch management, MaaS360 allows the configuration of DO, enabling peer-to-peer updates in which networked Windows endpoints supply some of the updates to other devices on the network rather than relying entirely on connection to Microsoft servers.

Device compliance & security

BYOD and data loss prevention (DLP)

Any corporate Windows 10 devices can make use of the DLP capabilities available through Windows Information Protection. As mentioned above, this feature allows organizations to designate as sensitive specific apps and data on a user's device. These items will then be encrypted and must first be decrypted each time a user goes to interact or view them. This is a feature available to all corporate-owned Windows 10 devices.

In the case of BYOD, however, these devices often run the Windows 10 Home operating system, which does not allow for WIP or most API-based policies. Regardless, MaaS360 can still support certain necessary security functions on these devices, including:

- Reporting on the service status, versions, and AV definitions of installed anti-virus, anti-spyware, and similar software
- Granular patch and update management as well as the ability to distribute any applications, files, or scripts
- Automated out-of-compliance rules and actions for devices missing patches or running an older version of Windows 10, among other possible parameters

Mobile Threat Defense (MTD)

Don't be fooled by the label, MTD protects Windows 10 as well. Beyond policy and compliance—and even beyond the reaches of Windows Defender—additional risks still threaten the security of your users, devices, and data. Whether man-in-the-middle attacks preying on poorly configured home and public Wi-Fi or increasingly convincing phishing emails, users are constantly vulnerable to a growing landscape of threats. Via leading MTD vendor, Wandera, MaaS360 delivers proactive threat identification and remediation, whether that means taking action when a user connects to risky networks, blocking a browser from ever hitting a phishing landing page, or even detecting the telltale device slowdowns common to cryptojacking.

Device compliance & security

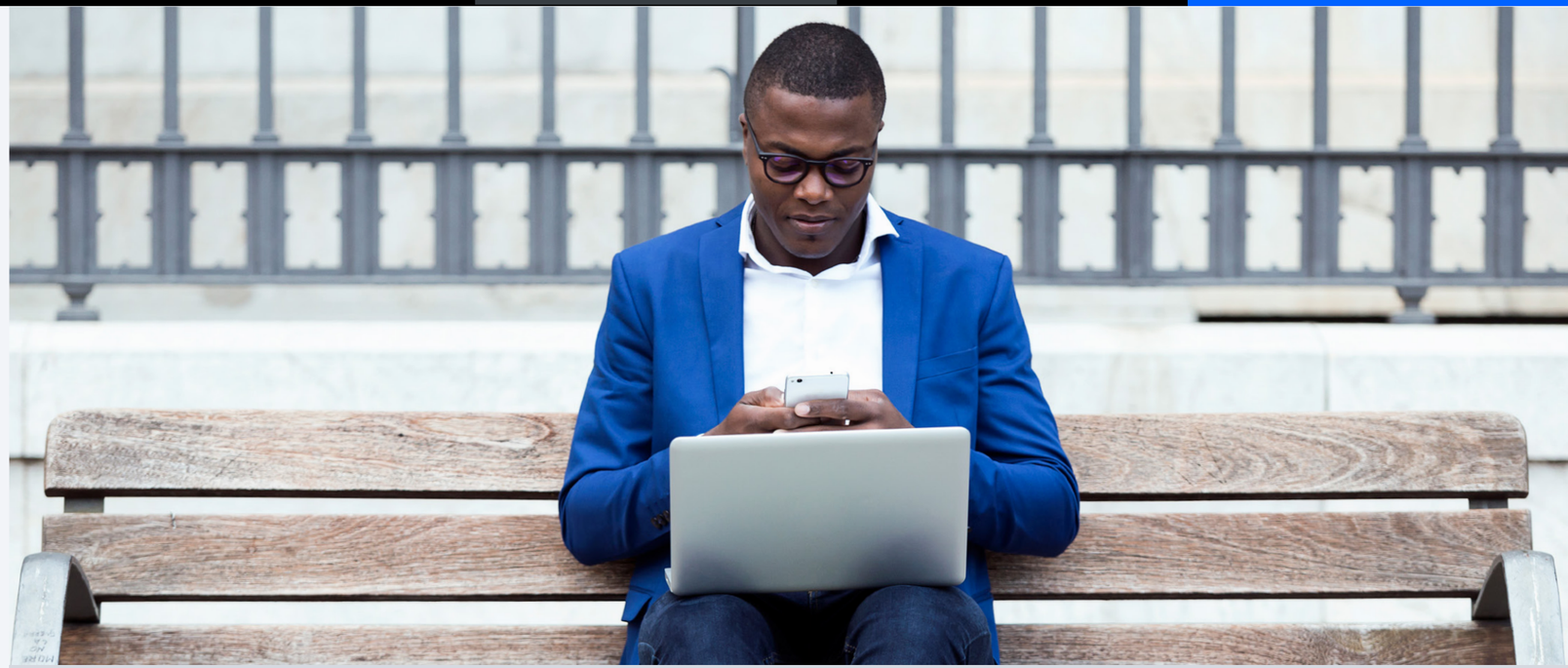
Identity and Access Management (IAM)
Deliver single sign-on (SSO) and multi-factor authentication (MFA) for cloud and enterprise apps via MaaS360 Identity, provided out-of-the-box through integration with IBM Cloud Identity. Used in conjunction with automated compliance rules, risk-based Conditional Access (CA) policies can be configured to ensure risky users are not interacting with sensitive data or other corporate resources.

Beyond this native workflow, MaaS360 and Identity can also be combined with an organization's existing SAML-based identity tools to again provide CA policies.

Beyond native identity features available within MaaS360, an organization's existing SAML-based identity tool can be integrated into the UEM deployment, either as the sole identity provider or in conjunction with the MaaS360 Identity feature to support conditional access.

TeamViewer remote support

At some point every user runs into an issue, whether something as simple as a forgotten passcode or a more complex connection or installation error. Ensure your users are well-supported from anywhere with TeamViewer and MaaS360. Through the MaaS360 console, launch TeamViewer and a remote session, either with the permission of the end user on an employee device or automatically for those endpoints unattended endpoints such as a kiosk or POS tablet.



Interested in learning more about what MaaS360 can do to support Windows deployments?

Start a trial

Ruggedized & IoT

Regardless of the specific use case, MaaS360 supports various ruggedized, wearable, and IoT devices to address line-of-business needs. Zebra, Bluebird, Panasonic, Kyocera, Honeywell, and M3 devices can be enrolled and have policies configured to enforce kiosk mode and distribute applications along with performing myriad other necessary functions.

Beyond this, MaaS360 supports non-standard deployments, from WatchOS to HoloLens to Android Things to Surface Hub interactive whiteboards. To learn more, read this case study detailing how one major pharmaceutical firm deployed 80,000 devices with MaaS360, 2,000 of which were IoT endpoints meant to support specific, mission critical processes.

Device compliance & security

Mobile Threat Defense (MTD)
Many IoT endpoints run on “mobile” operating systems such as Android or Windows 10, allowing MTD to maintain security and device integrity. Via leading MTD vendor, Wandera, MaaS360 delivers proactive threat identification and remediation, whether that means taking action when a user connects to risky networks, blocking a browser from ever hitting a phishing landing page, or even detecting the telltale device slowdowns common to cryptojacking.

Identity and Access Management (IAM)
Deliver single sign-on (SSO) and multi-factor authentication (MFA) for cloud and enterprise apps via MaaS360 Identity, provided out-of-the-box through integration with IBM Cloud Identity. Used in conjunction with automated compliance rules, risk-based Conditional Access (CA) policies can be configured to ensure risky users are not interacting with sensitive data or other corporate resources.

Beyond this native workflow, MaaS360 and Identity can also be combined with an organization’s existing SAML-based identity tools to again provide CA policies.

Beyond native identity features available within MaaS360, an organization’s existing SAML-based identity tool can be integrated into the UEM deployment, either as the sole identity provider or in conjunction with the MaaS360 Identity feature to support conditional access.

TeamViewer remote support

At some point every user runs into an issue, whether something as simple as a forgotten passcode or a more complex connection or installation error. Ensure your users are well-supported from anywhere with TeamViewer and MaaS360. Through the MaaS360 console, launch TeamViewer and a remote session, either with the permission of the end user on an employee device or automatically for those endpoints unattended endpoints such as a kiosk or POS tablet.

Interested in learning more about what MaaS360 can do to support non-traditional and IoT deployments?

Start a trial