baramundi

Whitepaper

Mobile Device Management Scenarios

How to optimize for COBO, COPE, BYOD and COSU

Empower your IT

CONTENTS

1 Modern Mobile Device Management

The use of mobile devices by employees has become common and expected at most companies, especially since the rapid growth of remote workforces. Users need and want to access company e-mail, data and documents as part of flexible, location-independent work arrangements. There are multiple benefits for productivity, talent recruitment and other areas to be sure, though mobile device security presents added risks and management tasks for IT departments. Mobile device deployments need to strike a balance between security and usability for both users and IT managers.

Effective mobile device management (MDM) follows a two-pronged approach built around an accurate inventory of all smartphones and tablets connecting to the corporate network, and risk-appropriate levels of IT control of device access, apps and configurations. That process can be clarified by applying four common MDM scenarios based on device ownership (user vs. company) and primary type of usage:

1.1 Corporate Owned Business Only (COBO)

Corporate Owned Business Only (COBO) devices prevent users from installing or using any personal apps or data. This offers the greatest degree of IT control with very strict policies prohibiting "accidental" personal use via jailbreaking, rooting or other methods. However, such restrictions can be inconvenient and unproductive, requiring users to carry and use two or more devices to accomplish everyday tasks. For example, they may get an urgent assignment via business email on their COBO phone, then grab their own device to send a WhatsApp message to friends or significant others to say they’re going to be working late. In many cases, such devices spend a lot of time in users’ backpacks or desk drawers.

1.2 Corporate Owned Personally Enabled (COPE) and Bring Your Own Device (BYOD)

Corporate Owned Personally Enabled (COPE) devices are issued to users for both business and private use and managed centrally in by the MDM system. This is usually accompanied by relatively relaxed user guidelines to make private use possible and practical. Employees often use a COPE device as their primary means of communication, enabling more seamless workflows with greater convenience and productivity. Data protection and user privacy concerns require that work and personal apps and data must be stored and managed separately in their own virtual containers.

Bring Your Own Device (BYOD) is exactly as the term implies, where users supply their own devices that they’ll also use for work after submitting it to IT for configuration and management. As with COPE devices, personal and business data must be stored and managed independently. IT managers also want to keep company data from intermingling with user data, e.g., the user’s WhatsApp account uploading company contacts or business-related data and metadata. At the same time, IT admins should not have any visibility on or access to the user's private apps and data, and users need to be assured that their personal info is protected from prying eyes.

1.3 Corporate Owned Single Use (COSU)

Corporate Owned Single Use (COSU) devices are configured exclusively for a specific use with only one app or a defined list of apps installed and authorized to run. Examples include mobile barcode scanners for delivery and warehouse logistics, or POS systems used by retail or restaurant staff. COSU devices also include menu and meal ordering systems for restaurant patrons or vehicle selection for customers at a car dealership. COSU tablets also are used in industrial settings for production data acquisition and machine data collection.

These devices are shared by multiple people so do not require user authentication. This also means that misuse cannot be attributed to a specific user. Device configuration must be well thought-out and restrictive in order to prevent unauthorized use and security breaches.

2 Ensuring Security

Smartphones and tablets are exposed to nearly the same threats as traditional PCs and laptops. In recent years, they've been facing targeted cyberattacks from an expanding array of malware. Choosing the right MDM solution begins by asking some important questions. Your answers will provide a solid starting point for defining your MDM requirements:

- How easy is it to add mobile devices to the MDM system?
- Can the devices be inventoried, how often, and to what level of detail?
- Can mobile devices be easily configured to meet specific needs?
- What security and user privacy functions are provided?
- Does it support platform-specific functions such as Apple Business Manager or Android Enterprise?
- Is it integrated with your other endpoint management systems and workflows?
- How usable and flexible is it for users and IT staff?

2.1 Enrollment

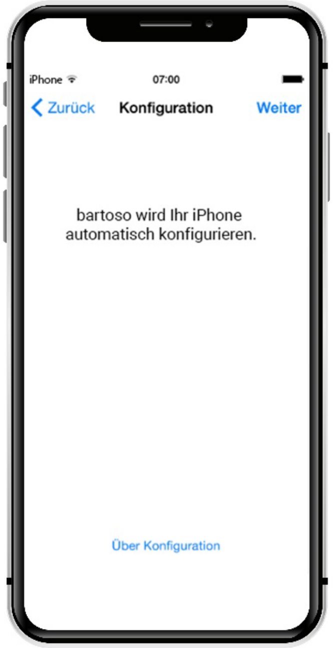
Mobile devices must first be enrolled, or added to and registered with the MDM server. iOS smartphones and tablets use the Apple Device Enrollment Program while Android devices use Android Enterprise Work Profiles.

2.1.1 Apple Device Enrollment Program (DEP)

Apple Business Manager provides an efficient and elegant way to add iOS devices to the MDM system using the Device Enrollment Program (DEP). IT administrators can use DEP to customize device configurations and define user authorizations during device activation. DEP gives IT administrators assurance that all company devices are appropriately managed.

2.1.2 DEP Set-up and Deployment

DEP also speeds device provisioning with bulk enrollment. End users receive their devices in their original packaging, pre-enrolled, under IT management and ready for use.

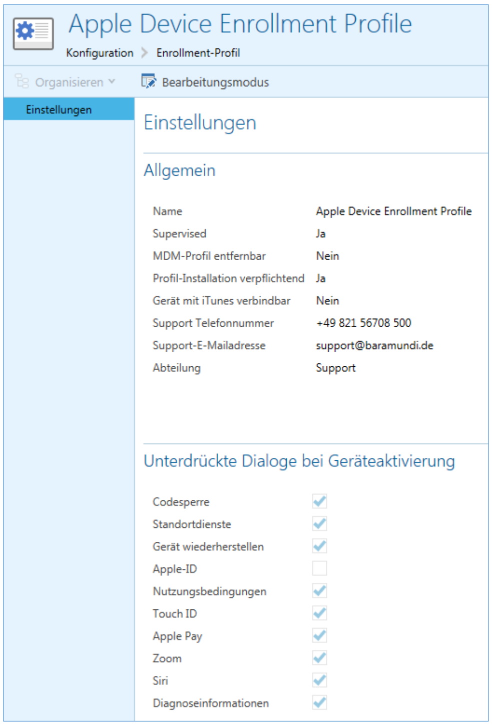


bartoso wird Ihr iPhone automatisch konfigurieren.

2.1.3 DEP from the Admin’s Perspective

IT administrators do not need physical access to the iOS device to integrate it securely into the MDM system. Instead, an admin can pre-configure a new COBO, COPE, BYOD or COSU device to ensure compliance with corporate policies as it is activated. An additional benefit is that all user rights and devices are configured within a simple profile and managed using consistent procedures.

User activation in DEP


Apple Device Enrollment Profile
Konfiguration > Enrollment-Profil
Organisieren
Bearbeitungsmodus
Einstellungen

Einstellungen

Allgemein

Name	Apple Device Enrollment Profile
Supervised	Ja
MDM-Profil entfernbar	Nein
Profil-Installation verpflichtend	Ja
Gerät mit iTunes verbindbar	Nein
Support Telefonnummer	+49 821 56708 500
Support-E-Mailadresse	support@baramundi.de
Abteilung	Support

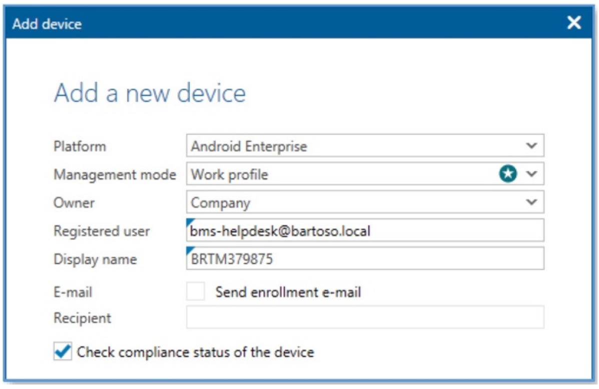
Unterdrückte Dialoge bei Geräteaktivierung

Codesperre	☑
Standortdienste	☑
Gerät wiederherstellen	☑
Apple-ID	□
Nutzungsbedingungen	☑
Touch ID	☑
Apple Pay	☑
Zoom	☑
Siri	☑
Diagnoseinformationen	☑

iOS Device Enrollment Profile

2.1.4 Android Work Profiles

Android devices can be “Fully Managed” for COBO or COSU or can use Work Profiles for COPE or BYOD smartphones and tablets. The mode for each device is defined during enrollment. The user installs the MDM management agent from the Play Store, adds it to management via a QR code, and receives instructions on how to use the Work Profile on their particular device.



Add a new device

Platform	Android Enterprise
Management mode	Work profile
Owner	Company
Registered user	bms-helpdesk@bartoso.local
Display name	BRTM379875
E-mail	□ Send enrollment e-mail
Recipient	

☑ Check compliance status of the device

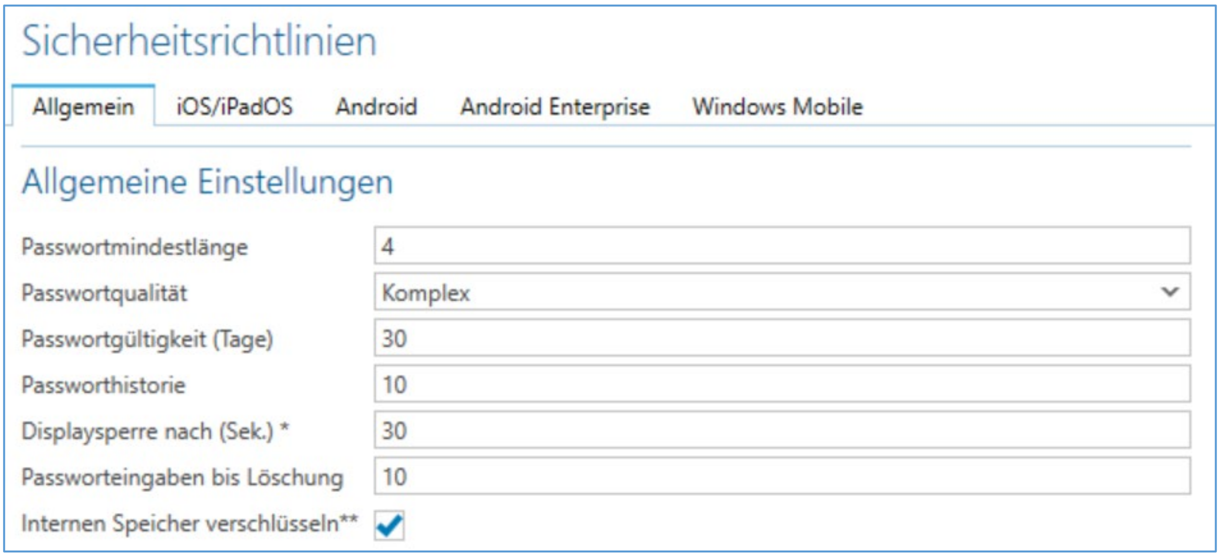
Enrollment dialog for the Work Profile

2.2 Inventory

The inventory functions of an MDM system are the foundation for ongoing device and security management. Accordingly, look for a system that monitors and displays detailed, up-to-date information on demand about hardware and security settings, installed apps and certificates and other data on every deployed device. Inventory functions also should include the ability to alert IT administrators and take automatic action on unauthorized device changes that pose serious security risks.

2.3 Password Policy Enforcement

Strong password protection to protect company data and prevent unauthorized access can be enforced on mobile devices with an MDM system. Password policies can be defined to can enforce company standards for password length, required characters and complexity. Device encryption policies also can be enabled as needed.



Sicherheitsrichtlinien

Allgemeine Einstellungen

Passwortmindestlänge	4
Passwortqualität	Komplex
Passwortgültigkeit (Tage)	30
Passworthistorie	10
Displaysperre nach (Sek.) *	30
Passworteingaben bis Löschung	10
Internen Speicher verschlüsseln**	☑

Configuration of a security profile

2.4 Remote lock, wipe and unlock

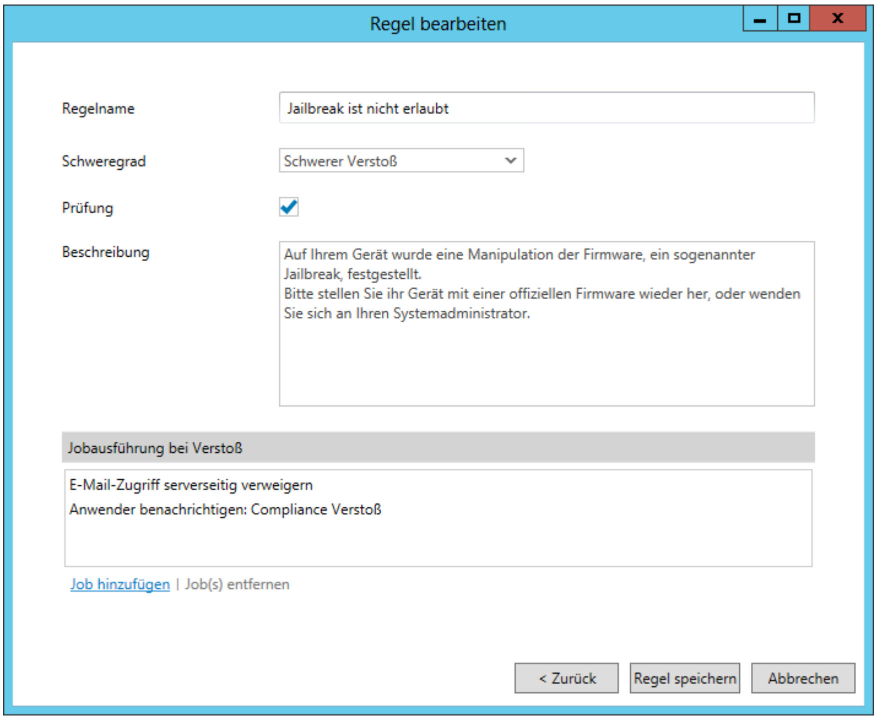
Generally speaking, lost mobile devices can be locked and wiped remotely. Depending on the device, an administrator can remotely perform a targeted data wipe (also known as "enterprise wipe" or "selective wipe") on company data only and leave user apps and data untouched. This makes BYOD device management easier to implement.

If the user forgets their password, the administrator can unlock the device remotely. Depending on the device, an administrator can disable biometric unlocking and require a PIN. An administrator also can also locate the device in "Lost Mode.”

2.5 Spotting Jailbreaks and Rooted Devices

The terms jailbreak (on iOS devices) or root (on Android) refer to aftermarket modifications to mobile device firmware. It’s usually done to enable a user to install applications from potentially unsafe sources such as unapproved app stores, to unlock functions disabled by the manufacturer or make other changes. Instructions on how to jailbreak or root mobile devices are widely available on the Internet.

From an MDM perspective, a jailbreak or a root can bypass the carefully defined management and security functions put in place by IT administrators and significantly increase the risks of malware or network intrusions. In addition, a device with unauthorized modifications limits IT's ability to manage or restore it to safe operation via the MDM system. For this reason, the MDM should continuously monitor mobile devices for tampering and automatically disable access to the company network.



Regel bearbeiten

Regelname: Jailbreak ist nicht erlaubt

Schweregrad: Schwerer Verstoß

Prüfung: ☑

Beschreibung: Auf Ihrem Gerät wurde eine Manipulation der Firmware, ein sogenannter Jailbreak, festgestellt.
Bitte stellen Sie ihr Gerät mit einer offiziellen Firmware wieder her, oder wenden Sie sich an Ihren Systemadministrator.

Jobausführung bei Verstoß

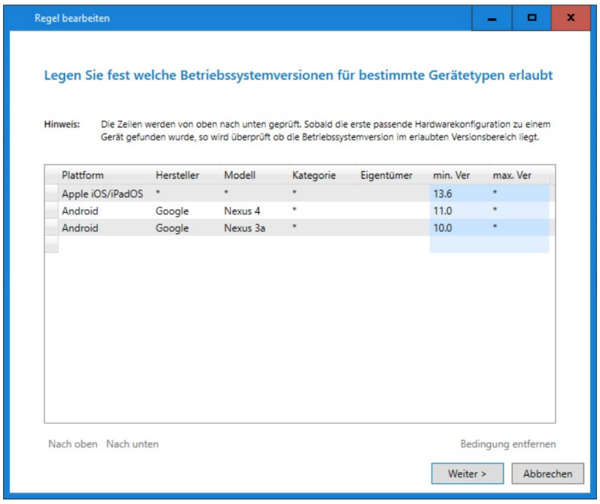
E-Mail-Zugriff serverseitig verweigern
Anwender benachrichtigen: Compliance Verstoß

Checking for Jailbreaks

2.6 Firmware Updates

Just as important as preventing firmware tampering is the prompt updating of device firmware to add new functions and improve performance and security. A good MDM not only ensures that devices receive firmware updates, it gives IT administrators greater control over the update process. For example, updates can be delayed by a specified period to allow for pre-deployment testing to spot and remedy potential incompatibilities with specialized in-house apps and device settings.

Continuous firmware status monitoring is possible through the MDM inventory function that includes an automatic cross-check of settings, apps and data on each device and company rules and policies.



Legen Sie fest welche Betriebssystemversionen für bestimmte Gerätetypen erlaubt

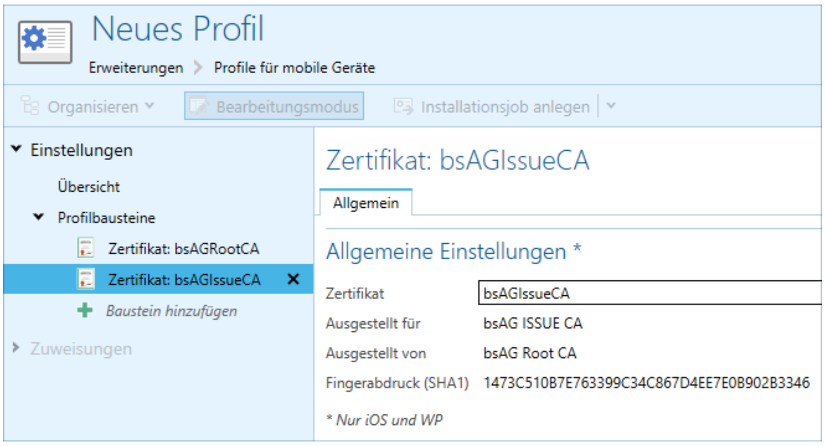
Hinweis: Die Zeilen werden von oben nach unten geprüft. Sobald die erste passende Hardwarekonfiguration zu einem Gerät gefunden wurde, so wird überprüft ob die Betriebssystemversion im erlaubten Versionsbereich liegt.

Plattform	Hersteller	Modell	Kategorie	Eigentümer	min. Ver	max. Ver
Apple iOS/iPadOS	*	*	*		13.6	*
Android	Google	Nexus 4	*		11.0	*
Android	Google	Nexus 3a	*		10.0	*

Checking rule for operating system versions

2.7 Security through Certificates, Distribution and Enterprise Wi-Fi

MDM security functions also should enable the distribution of client enterprise certificates and be able to support the necessary trust positions against enterprise services.



Zertifikat: bsAGIssueCA

Ausgestellt für: bsAG ISSUE CA

Ausgestellt von: bsAG Root CA

Fingerabdruck (SHA1): 1473C510B7E763399C34C867D4EE7E0B902B3346

* Nur iOS und WP

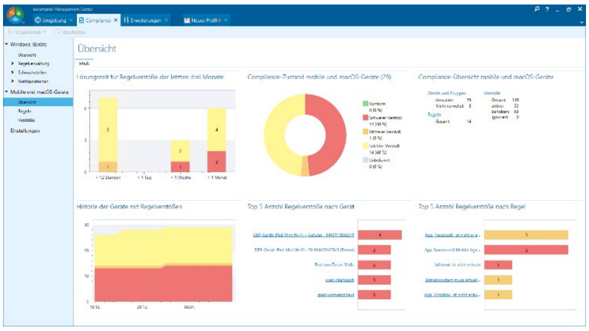
Profile module for client certificates

Such certificates are used in place of user logins to, for example, secure access to Microsoft Exchange or to support secure enterprise Wi-Fi.

2.8 Compliance and IT Policies

It’s especially important to ensure compliance with company rules regarding authorized and unauthorized apps. In addition to blocking lists for apps or the detection of firmware modifications, compliance policies also can check for and install required apps that are missing.

Compliance information should be displayed on an administrator’s dashboard and sorted by device types or the severity of compliance violations to show at a glance where immediate action is required. A good MDM also will enable automated responses such as notifying the user via email or remotely wiping and locking a device in the event of particularly serious violations such as a jailbreak or root.


baramundi Management Center
Umgebung
Compliance
Erweiterungen
Neues Profil
Organisieren
Bearbeiten
Windows Geräte
Übersicht
Regelverwaltung
Schwachstellen
Konfigurationen
Mobile und macOS-Geräte
Übersicht
Regeln
Verstöße
Einstellungen
Übersicht
Inhalt
Lösungszeit für Regelverstöße der letzten drei Monate
< 12 Stunden
< 1 Tag
< 1 Woche
< 1 Monat
Compliance-Zustand mobile und macOS-Geräte (29)
Konform 0 (0 %)
Schwerer Verstoß 14 (48 %)
Mittlerer Verstoß 1 (3 %)
Leichter Verstoß 14 (48 %)
Unbekannt 0 (0 %)
Compliance-Übersicht mobile und macOS-Geräte
Geräte und Gruppen
Verwaltet 29
Nicht verwaltet 8
Regeln
Gesamt 14
Verstöße
Gesamt 119
aktive 50
behoben 69
ignoriert 0
Historie der Geräte mit Regelverstößen
Top 5 Anzahl Regelverstöße nach Gerät
iPad von Öscan Walk
Top 5 Anzahl Regelverstöße nach Regel
App 'baramundi Mobile Age...
Jailbreak ist nicht erlaubt
Betriebssystem muss aktuell...

IT Policy Dashboard

3 Conclusion

Selecting the best MDM solution includes more than just picking one with the capabilities needed to support the desired deployment of COBO, COPE, BYOD or COSU devices. It also entails choosing one that meets the needs of IT staff and users. This is a subtle but important consideration that can determine not the ultimate success of your company's mobile device deployment. IT managers should look for a balance of:

- Support for business security requirements
- The user experience for employees
- A consistent, intuitive interface for IT staff with easily customizable automation functions.

A final factor is to precisely define the required scope of functions. It is often advisable to go beyond the capabilities of MDM and consider systems that also integrate Mobile Application Management (MAM) as part of a comprehensive Enterprise Mobility Management (EMM) solution.

You can find more information in our EMM whitepaper and our webinars.

About baramundi Software

baramundi Software enables companies and organizations to efficiently, securely and cross-platform management of workplace environments. More than 4,000 customers of all industries and sizes worldwide benefit from the German manufacturer's many years of experience and excellent products.

These are combined in the baramundi Management Suite according to a holistic, future-oriented unified endpoint management approach: Client management, mobile device management and endpoint security are carried out via a common interface, in a single database and according to uniform standards.

By automating routine work and comprehensively overview of the state of all end points, the baramundi Management Suite optimizes IT management processes. It relieves IT administrators and ensures that users have the rights and applications they need on all platforms and form factors, on PCs, laptops, or mobile devices, anytime, anywhere.

The headquarters of baramundi software AG are located in Augsburg. The products and services of the company, which was founded in 2000, are completely Made in Germany. baramundi works successfully with partner companies worldwide for the sales, consulting and support of users.

More information about baramundi: www.baramundi.com Would you like to view the EMM solution? Sign up for the live webinar See how you can manage smartphones and tablets as easily and reliably as PCs and notebooks: www.baramundi.com/de-de/webinare/enterprise-mobility-management/

Wir freuen uns Sie kennenzulernen!

Kontaktieren Sie uns!

baramundi software AG
Beim Glaspalast 1
86153 Augsburg, Germany

🇩🇪 +49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

🇬🇧 +44 2071 93 28 77
request@baramundi.com
www.baramundi.com

🇵🇱 +48 735 91 44 54
request@baramundi.com
www.baramundi.com

🌍 +49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 401
Framingham, MA 01701, USA

🇺🇸 +1 508 808 3542
requestUSA@baramundi.com
www.baramundi.com

baramundi software Austria GmbH
Landstraßer Hauptstraße 71/2
1030 Wien, Austria

🇦🇹 +43 1 7 17 28 - 545
request@baramundi.com
www.baramundi.com

Empower your IT