



Enterprise Mobility Management

What can management solutions achieve today?

CONTENTS

1	Enterprise Mobility Management (EMM).....	2
2	Automatic Management and Guaranteed Security	3
2.1	Enrollment.....	3
2.2	Inventory	3
2.3	Force Password Protection.....	3
2.4	Lock and Erase Remotely.....	4
2.5	Jailbreak and Root Detection.....	4
2.6	Firmware Update	5
2.7	Blacklisting and Whitelisting of Apps	6
2.8	App Configuration	7
2.9	Security Through Certificates, Deployment, and Enterprise Wi-Fi.....	9
2.10	Check IT Compliance	9
2.11	Offer Self-Service Options	10
2.12	Apple Device Enrollment Program (DEP)	10
2.13	Apple Volume Purchase Program (VPP).....	13
3	Extensive, Efficient, and Simple	15
3.1	Integrated vs. Standalone: What is Suitable for Whom?	15
3.2	Implementation Effort and Ease of Use of a Solution	15
3.3	Challenge of Platform Diversity	15
3.4	Transparent Management in Real Time	17
4	Checklist of Important Functions.....	18
5	Summary.....	20

© 2017 baramundi software AG

Statements regarding equipment and technical functionalities are not binding and are for information only.
Subject to change without notice. DocID WP-EMM-170616

Management Board: Uwe Beikirch, Dipl.-Ing. (FH) | Dr. Lars Lippert

Chairman of the Supervisory Board: Dr. Dirk Haft

Registered office and court: Augsburg, Commercial Register (HRB) no. 2064 | Tax ID number DE 210294111

1 Enterprise Mobility Management (EMM)

The use of mobile devices has become standard in many companies, and many employees want to access company data using their own mobile devices. This can offer some advantages for companies, but the IT managers should be aware of the risks. In order to integrate notebooks, tablets, and smartphones securely into everyday work, effective protection including inventory is a basic requirement.

Smartphones and tablets are, after all, portable computers and are exposed to virtually the same threats as desktop PCs. In 2016, mobile systems were bombarded with viruses. Experts recorded so many more different types of malware than ever before. It revealed a new trend: mobile malware is increasingly copying the functions and effects of malware on the desktop. Companies need to arm themselves against this.

When companies initially consider a mobility strategy and the introduction of EMM software in this regard (as an addition to endpoint management or as a standalone EMM suite), there are some important questions to answer first in order to find the right solution.

- How easy is it to include mobile devices in the management solution?
- Can the devices be inventoried?
- Can mobile devices be configured with the solution?
- Which security functions should the EMM solution offer?
- Does the EMM solution support special business functionalities such as the Apple Volume Purchase Program?
- Integrated vs. standalone: which solution is right for whom?
- How easy is it to use the software?
- Can heterogeneous operating systems be managed efficiently?

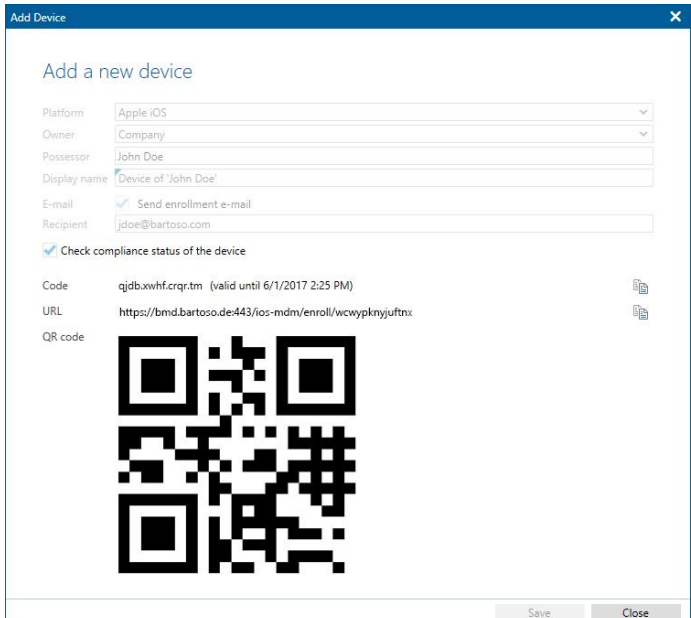
This creates a personal requirements list, which forms the basis for considering the various providers in more detail and preselecting suitable solutions. Based on this individual shortlist, administrators should then test and evaluate EMM suites in practice.

The objective of managing mobile devices is the same as that for PC clients: to effectively ensure disruption-free operation, always maintain an overview of the status of the devices, and guarantee security. Mobile devices can be comprehensively managed and secured using an Enterprise Mobility Management solution.

2 Automatic Management and Guaranteed Security

2.1 Enrollment

For an EMM solution to be used for management, the relevant mobile devices must first be recorded in the solution and logged in to the management server. Enrollment should be simple and, as far as possible, should also be possible via a network connection for a user without any IT knowledge – especially if a Bring Your Own Device scenario is to be implemented. An example: The administrator generates a QR code and sends it by email to a user. The user scans the code on their screen with the new smartphone, confirms the management by the EMM suite, and the device can be managed from then on.



Enrollment with baramundi Mobile Devices

2.2 Inventory

Which devices can be found in my network and what has been installed on these devices? An EMM solution should be able to provide basic answers to these questions for all popular operating system platforms. With the solution, information on the hardware and security settings, as well as the installed apps and certificates, can be collected on iOS, Android, and Windows mobile devices.

2.3 Force Password Protection

To secure valuable company data, a strong password is required for reliable protection against unauthorized access. This can be forced on the mobile platforms with an EMM solution. Here it is possible to specify the complexity of the password in order to prevent the user from using a simplistic or non-secure combination (e.g. "1234"). Guidelines for device encryption can be activated subsequently if they are not already active.

Security policies

Common
iOS
Android
Windows Phone

General settings

Minimum password length	6
Password quality	complex
Password validity (days)*	30
Password history*	10
Display timeout (sec)	60
Password retries before device wipe	10
Encrypt internal storage*	<input checked="" type="checkbox"/>

* on Android not before V3.0

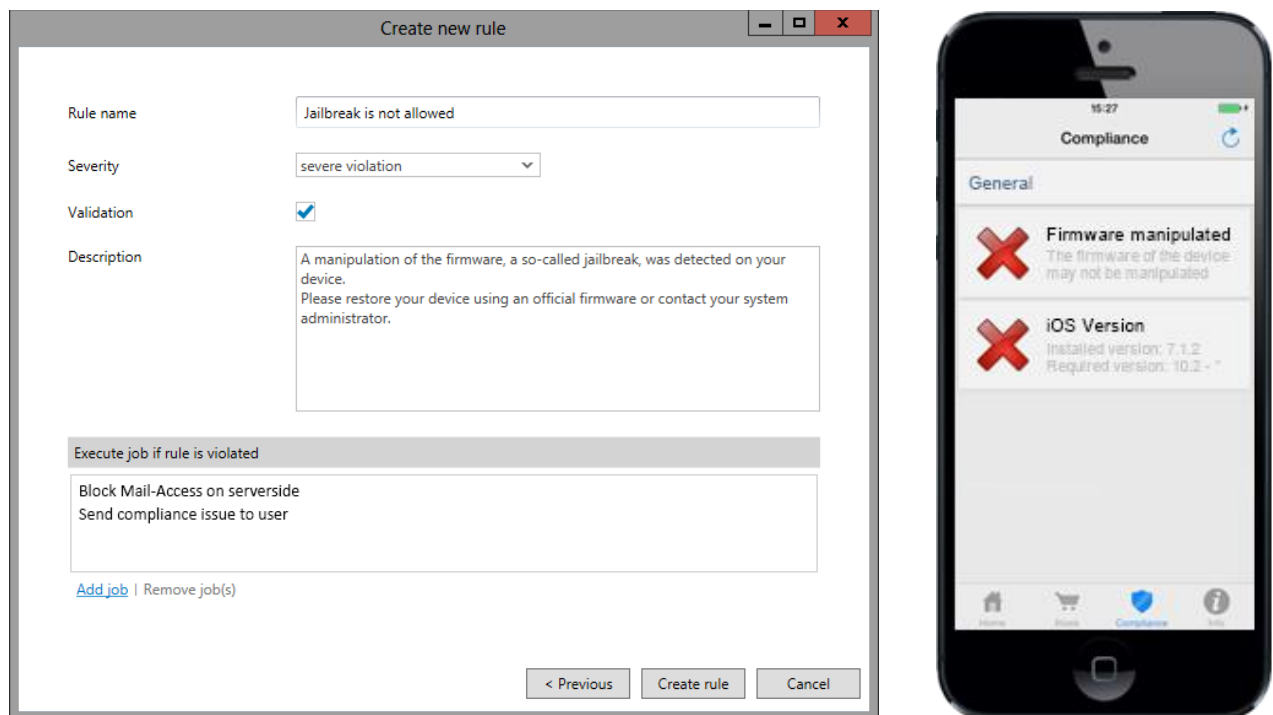
Configuration of a security profile

2.4 Lock and Erase Remotely

If the device is lost, depending on the platform, devices can be locked and erased remotely. If the user forgets their password, the administrator can help to unlock the device remotely.

2.5 Jailbreak and Root Detection

Jailbreaking (in iOS devices) or rooting (in Android) means the modification of the firmware in a mobile device. These modifications allow the user to install applications or activate functions which are not provided or approved by the manufacturer, for example. Instructions for this circulate online. A jailbreak or rooted smartphone renders the protective functions of the operating system ineffective. The risk of getting malware increases significantly. In addition, the management of an unlocked device using the EMM solution is only possible to a limited degree, because its security functions can be circumvented. Therefore, companies should always have suitable compliance checks in place to prevent such a modification.

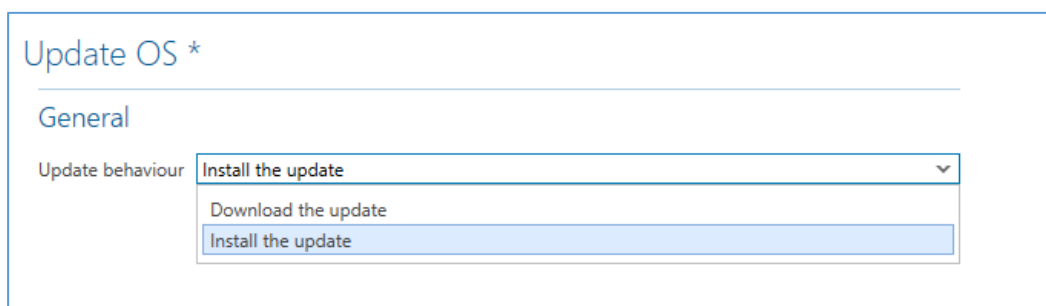


Checking for jailbreaks

For security reasons, devices modified in this way are viewed as extremely critical. Such interventions should be detected by an EMM solution. The end user can also be shown this type or other types of compliance violation using a connected management app.

2.6 Firmware Update

Updating firmware as soon as the manufacturer provides a new version is just as important as preventing firmware manipulations. As a rule, updates don't just offer new functions, but also eliminate vulnerabilities. These upgrades can already be controlled remotely on modern platforms.



Operating system update using remote control

Monitoring the firmware status is possible on all platforms. The administrator can see an overview remotely at all times by using an inventory or – a more elegant solution – smart compliance rules that are checked automatically.

Create new rule

Please define which OS versions are allowed for certain device types

Note: The lines will be checked from top to bottom. As soon as a matching hardware configuration for a device is found, it will be checked if the OS version is in the allowed version range.

Platform	Manufactur...	Model	Category	Owner	min. ver	max. ver
Android	samsung	Galaxy S7	*		6.0	*
Apple iOS	*	*	*		10.2	*
Windows Phone	Microsoft	Lumia 950 XL	*		10.0	*

Up

Down

Remove condition

Next >

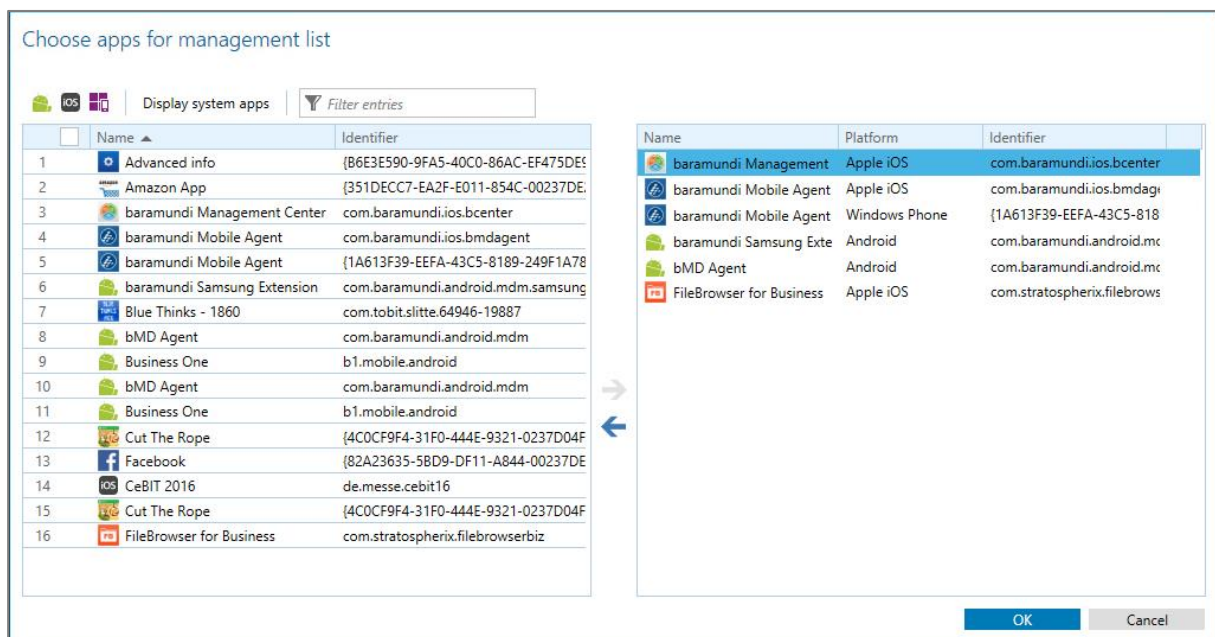
Cancel

IT compliance rules for operating system versions

2.7 Blacklisting and Whitelisting of Apps

In order to prevent dangerous apps from being run or to offer a selection of apps that the company classifies as trustworthy, the solution should support blacklisting and whitelisting of apps. This enables the administrator to prevent unwanted apps from being installed or run on compatible mobile devices. Conversely, whitelisting enables expressly permitted apps to be defined so that all apps not listed are prevented from being installed or run.

Depending on the preference of the administrator, either whitelisting or blacklisting can be used for an end device. Following the decision on which type of list, the required apps are added to the list and then transferred as the profile to the mobile device.



App selection for blacklisting and whitelisting

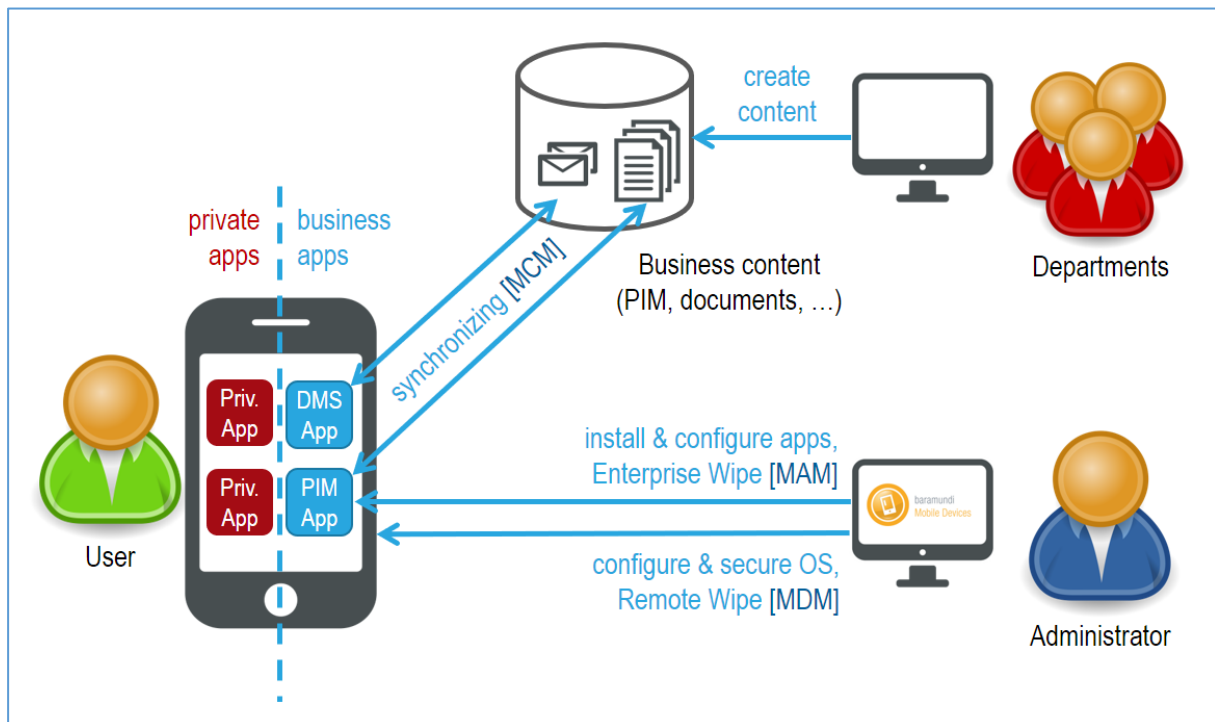
Using a suitable EMM solution, the administrator can also see at a glance whether or not a previously installed app can be run. The company can use these app lists for effective protection against malware apps.

2.8 App Configuration

Enterprise Mobility Management is an umbrella term encompassing several subdisciplines that deal with the management of mobile devices. The three key components here are Mobile Device Management (MDM), Mobile Application Management (MAM), and Mobile Content Management (MCM) – namely the management of the device as a whole, the individual apps installed on it, and the content it holds. How does the baramundi solution support holistic EMM?

As an active member of the AppConfig Community, an initiative launched by leading EMM solution providers, baramundi aims to simplify the deployment and configuration of apps by leveraging the native capabilities provided by operating system manufacturers. The suite offers a multitude of MDM and MAM functions, and is supplemented with MCM functions via suitable apps from third-party providers in the DMS/PIM field. Configuration standards at the iOS or AppConfig level allow these areas to be combined, ensuring that the bMD solution takes care of the straightforward deployment and setup of the MCM functions, while the functions they contain – for example data synchronization with selected backend systems, and data visualization/editing – are reserved for the third-party apps. This best-of-breed approach

brings MDM/MAM and MCM together into a comprehensive EMM solution. The following diagram clarifies these relationships between elements by depicting typical mechanisms.



$$MDM + MAM + MCM = EMM$$

The **administrator** uses the MDM and MAM features of baramundi Mobile Devices to first configure and secure employees' mobile devices, and then to install and configure business apps. The specific MCM functions will then be provided by the relevant third-party apps, which are also deployed and suitably configured at the same time with baramundi Mobile Devices. This configuration includes the preallocation of user names, connection paths to server systems, and many other detailed app settings.

If an end device gets lost, the administrator is able to use appropriate apps to remotely perform a targeted data wipe on the app (also known as "enterprise wipe" or "selective wipe"). This function makes BYOD concepts easier to implement.

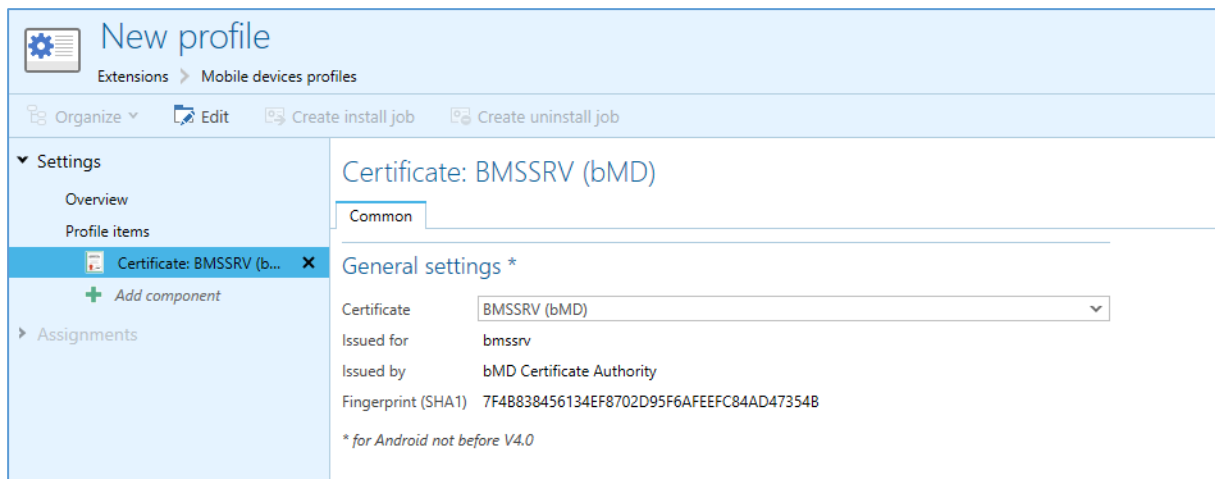
The **user** can use, in addition to the standard operating system tools, special container apps for PIM (personal information management, i.e. emails, calendar, contacts, etc.) or document management, which help to visualize content and enable synchronization with backend systems. In addition to these functions, these apps also provide additional security features, in order to encrypt data stored there and keep business data separate from private data in the context of BYOD policies.

The **departments** (including the mobile device user mentioned above) continue to use the applications they are familiar with to store content in business solutions. Business solutions

can be anything from PIM systems like Microsoft Exchange to file storage locations such as SharePoint, WebDAV, and various cloud storage solutions for business.

2.9 Security Through Certificates, Deployment, and Enterprise Wi-Fi

An EMM solution should also facilitate the deployment of client company certificates and be able to support the required trust chains with regard to company services.



Profile element for endpoint certificates

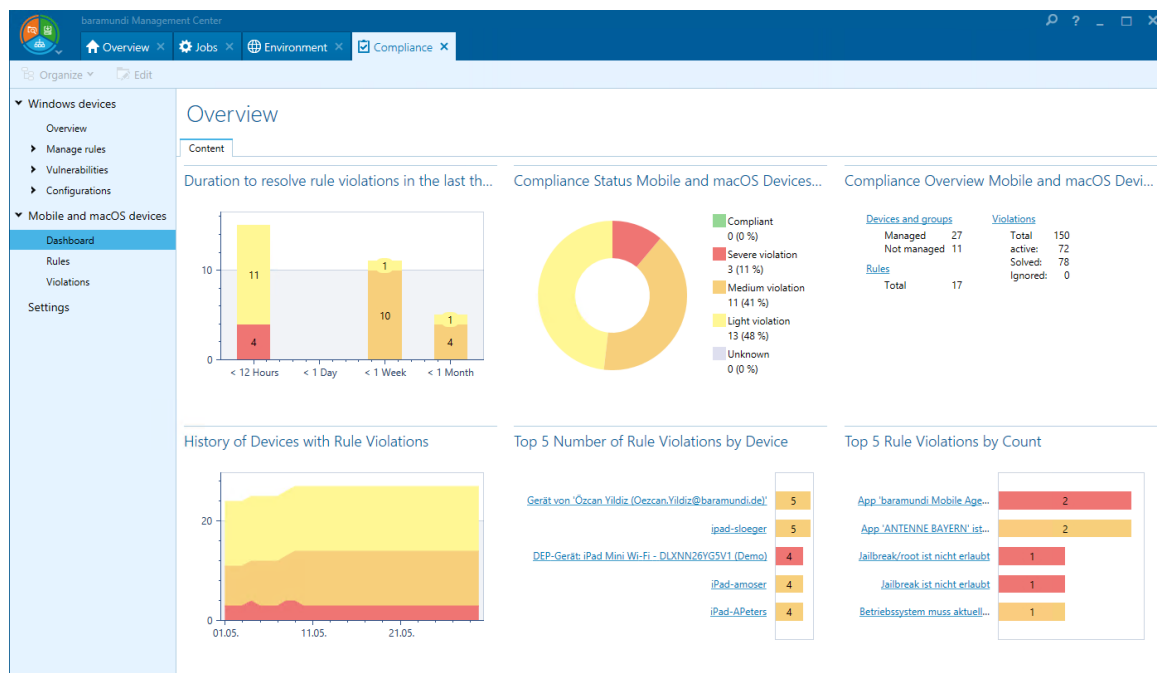
These certificates can be used to safeguard access to Microsoft Exchange or implement the WLAN in the form of secure Enterprise Wi-Fi. Both secure the connection by certificate instead of user credentials.

2.10 Check IT Compliance

It is particularly important to ensure mobile devices comply with the company's IT rules. Security requirements can be enforced by blacklisting and whitelisting apps and detecting jailbreaks or roots. For example, the EMM solution should identify if specifically required apps are missing from a device.

Information about the state of compliance should be displayed as an overview on a dashboard sorted according to device or severity of infringement. The administrator can tell at a glance what urgently requires attention. EMM solutions are recommended that facilitate automated responses to these – from emailing the user through to remote wiping of a device if there are especially severe infringements, such as a jailbreak.

With baramundi Management Suite, it is also possible to give the user the option to access the compliance status of their own smartphone or tablet in the self-service area.



Dashboard for IT compliance

2.11 Offer Self-Service Options

Self-service solutions are an elegant option, which gives the user immediate support and simultaneously reduces the flow of support queries. Pre-prepared administration jobs are available in a Kiosk area, which runs fully automatically and without intervention by the administrator when called up by a user. Users can then install store apps and company apps independently, or they are taken to the corresponding app in the store. Configuration settings can also be offered in this way.

2.12 Apple Device Enrollment Program (DEP)

With the introduction of the Device Enrollment Program (DEP), Apple is providing efficient methods of integrating new iOS devices quickly and elegantly into the management of an EMM solution.

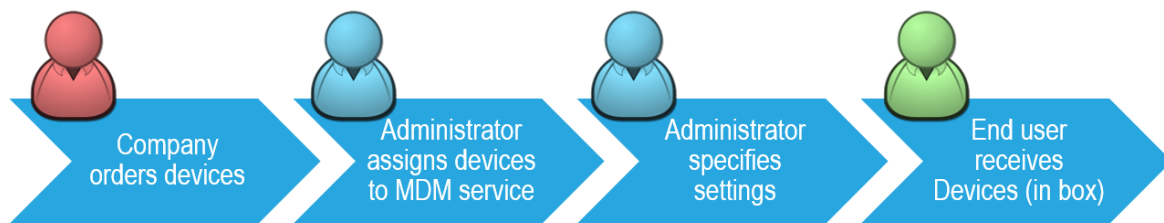
It is advisable to select an EMM solution that supports these options and permits direct enrollment. The administrator can adapt this process to suit his or her personal preferences using the configuration by defining the degree of freedom end users have during the activation phase of the device.

DEP benefits end users by allowing them to activate devices more quickly and simply. The company also benefits with increased security: The administrator uses new settings to ensure

that a company device is always managed. In particular, the administrator can prevent management profiles from being removed from iOS devices by the end user.

2.12.1 The DEP provision process

Apple's DEP enables the following simplified provision processes within an EMM solution, which accelerate setup and also offer elegant mass enrollment.



Provision process for iOS devices

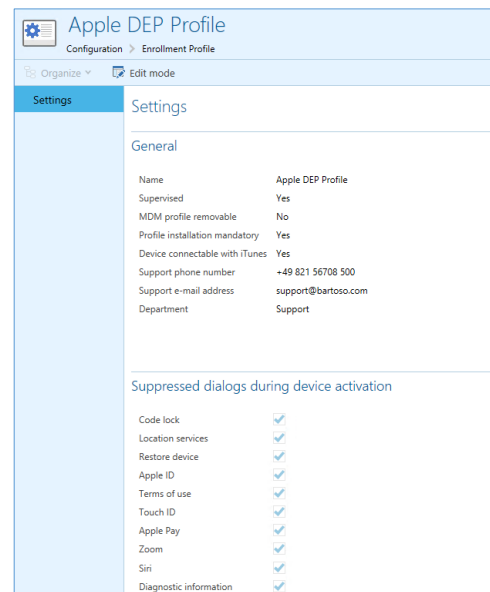
The company orders the iOS devices from Apple or another retailer or phone provider authorized for DEP. Before delivery, the devices are assigned to the EMM service by the administrator and configuration settings are made in the EMM solution. The end user thus receives the devices in their original packaging with immediate management connection at the time of device activation.

2.12.2 DEP from the administrator's perspective

The administrator no longer needs physical access to the iOS device in order to securely integrate it in the Enterprise Mobility Management.

With an EMM solution, they can preconfigure the new device in order to ensure that it complies with company guidelines during activation. They can prevent the user from removing the device from management and ensure that all users have the same device configuration.

The administrator defines the desired properties and degree of freedom of the end user during activation within a simple profile.



iOS Device Enrollment profile

2.12.3 DEP from the end user's perspective

DEP makes the activation process for a newly received iOS device significantly easier for the end user. Instead of the variety of dialog pages that the user previously had to answer in the course of activation, the administrator's preconfiguration now improves the degree of automation.

The appropriate preconfiguration reduces the number of user questions and increases security. This simplification affects not only initial commissioning but also the installation of apps, so that in connection with VPP (see below), wanted apps find their way onto the device without the hassle of query dialogs.



iOS activation with DEP

2.13 Apple Volume Purchase Program (VPP)

For businesses, Apple is continuing to develop the Volume Purchase Program (VPP) for the purchase and management of Apple app licenses, and offers the administrator alternative uses in parallel. In addition to the app purchase using VPP redemption codes, the EMM solution should also support the app distribution using Managed Distribution Client Assignment. Licenses can be purchased for devices and assigned to them instead of having to couple licenses to users' Apple IDs.

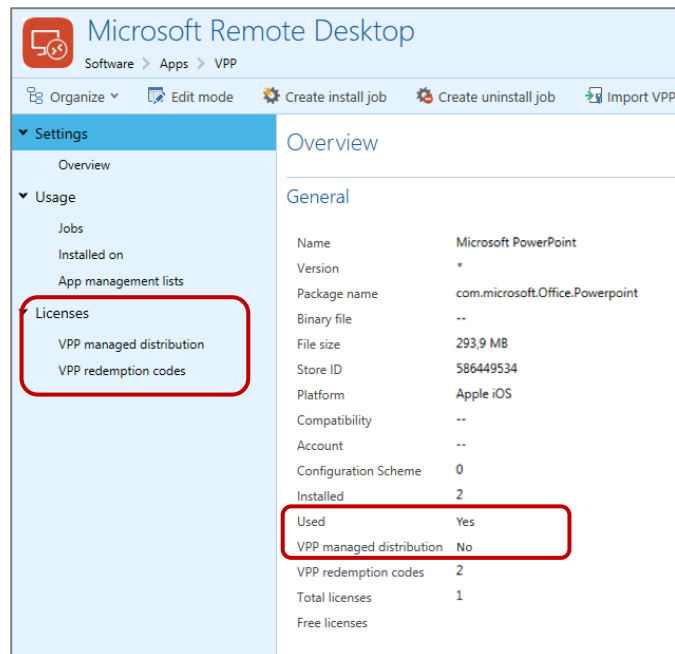
	VPP Redemption Codes	VPP Managed Distribution User Assignment	VPP Managed Distribution Client Assignment
Linking of licenses	Apple ID*	Apple ID*	Device
Deployment of free and chargeable apps	only with Apple ID*	only with Apple ID*	without Apple ID*
Deployment without user interaction	n/a	n/a	yes (for supervised devices)
Handling of licenses / display in the MDM suite	list of licenses; manual input	automatic association in the MDM suite	automatic association in the MDM suite
Withdrawal of licenses by the administrator	n/a	yes	yes
Availability from Apple	iOS 5	iOS 7	iOS 9

*) "Apple ID" denotes the ID of the end user with regard to Apple

2.13.1 VPP support from the administrator's perspective

VPP support offers different options for the deployment of chargeable and free apps. For this, the administrator can choose between the use of redemption codes or managed distribution, individually for each app.

If the licenses are assigned to a device, they can also be unassigned for use on another device.



VPP support in bMD

3 Extensive, Efficient, and Simple

3.1 Integrated vs. Standalone: What is Suitable for Whom?

The way the solution is integrated into the existing corporate IT is a key decision. There is a choice between EMM solutions integrated in a unified endpoint management (UEM) suite, and EMM standalone solutions. Companies that opt for UEM software can often use it to manage mobile devices as well. The advantage here is obvious: if the EMM is integrated into unified endpoint management, then all endpoints can be managed centrally using one interface and the administrator has a complete overview. This is particularly suitable for companies that only have one or a small number of IT administrators who are responsible for the IT infrastructure as they can benefit from the synergy effects. Even though the functional scope may appear somewhat smaller compared to pure EMM suites, as a rule, the most important functions such as inventorization, configuration options, and the deployment of apps and security settings are covered.

3.2 Implementation Effort and Ease of Use of a Solution

When deciding on EMM software, administrators should note the effort required for implementation, commissioning, and training. It should be as easy as possible to integrate the suite into the existing IT landscape. It is also important that the solution is intuitive to operate and has a clear interface. This means that new co-workers or stand-ins can quickly learn how to use the EMM suite. And another benefit: extensive training creates additional costs – and IT departments already have to economize as budgets are often limited.

3.3 Challenge of Platform Diversity

Administrators are often required to support different mobile platforms, i.e. to understand them down to the details of their configuration, set them up, and support them. That is not only complex, but also requires a lot of time.

Taking as an example the Exchange configuration for receiving emails on the three popular mobile platforms Android, iOS, and Windows Mobile, it is clear that the same parameters (name, email address, domain, server, and encryption) always have to be entered in different dialogs, if this information is input manually.



Cancel Next

Email apple.fan@bartoso.com

Server mail.bartoso.com

Domain bartoso.com

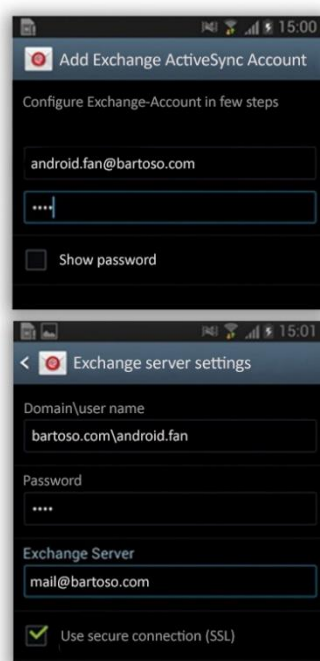
Username toook

Password

Account Advanced Settings

Use SSL ☒

iOS



Add Exchange ActiveSync Account

Configure Exchange-Account in few steps

android.fan@bartoso.com

.....

☐ Show password

Exchange server settings

Domain\user name
bartoso.com\android.fan

Password
.....

Exchange Server
mail@bartoso.com

☒ Use secure connection (SSL)

Android



OUTLOOK

Email address
windows.fan@bartoso.com

Password
.....

☐ Show password

User name
windowsfan

Domain
bartoso.com ?

Server
mail.bartoso.com ?

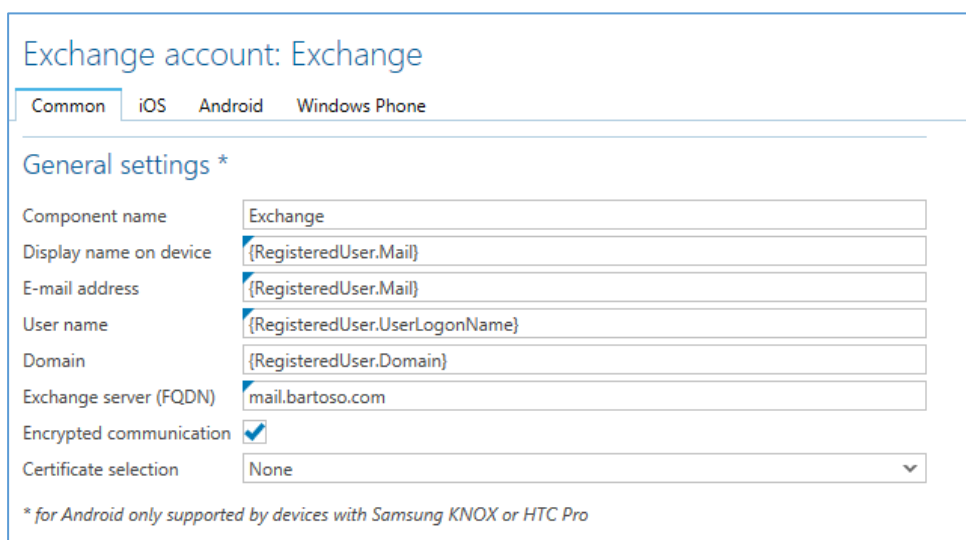
☒ Server requires encrypted (SSL) connection

Account name
bartoso

Windows 10 Mobile

Exchange configuration on different mobile platforms

There is therefore an obvious need for a tool which facilitates a standardized input for all devices to be managed. With an Enterprise Mobility Management solution like baramundi Management Suite, the administrator can manage all mobile devices uniformly from one interface. For example, this enables an Exchange configuration to be managed quickly and easily for different operating systems.



Exchange account: Exchange

Common iOS Android Windows Phone

General settings *

Component name Exchange

Display name on device {RegisteredUser.Mail}

E-mail address {RegisteredUser.Mail}

User name {RegisteredUser.UserLogonName}

Domain {RegisteredUser.Domain}

Exchange server (FQDN) mail.bartoso.com

Encrypted communication ☒

Certificate selection None

* for Android only supported by devices with Samsung KNOX or HTC Pro

Cross-platform Exchange configuration using an EMM suite

3.4 Transparent Management in Real Time

Good EMM software not only provides all relevant data about the managed mobile devices clearly, but should also make it available in real time, as far as possible. The administrator is only sufficiently informed when they have all the important information and responses in real time, and they can then assess the security of the mobile devices correctly. Job-oriented mechanisms score points here compared to rule-based paradigms. If there is a database that is constantly up-to-date, current reports can be exported and processed when required.

4 Checklist of Important Functions

Software deployment and configuration	
<input type="checkbox"/>	Distribution of firmware updates
<input type="checkbox"/>	Installation of apps with without user confirmation
<input type="checkbox"/>	Uninstallation of apps with without user confirmation
<input type="checkbox"/>	Support for Apple Volume Purchase Program (VPP)
<input type="checkbox"/>	Support for Apple Device Enrollment Program (DEP)
<input type="checkbox"/>	Installation uninstallation with deactivated App Store
<input type="checkbox"/>	Installation uninstallation of custom-made company apps
<input type="checkbox"/>	Self-Service App: Kiosk
<input type="checkbox"/>	Installation uninstallation of certificates
<input type="checkbox"/>	Parameterization of settings using variables
<input type="checkbox"/>	Installation of hyperlinks (iOS: Web Clip)
<input type="checkbox"/>	Deactivation of the camera
<input type="checkbox"/>	Configuration of access points (APN)
<input type="checkbox"/>	VPN settings

Inventory	
<input type="checkbox"/>	Hardware information
<input type="checkbox"/>	Configured restrictions (e.g. iCloud lock and similar)
<input type="checkbox"/>	Installed profiles
<input type="checkbox"/>	Installed certificates
<input type="checkbox"/>	SIM information
<input type="checkbox"/>	Roaming status
<input type="checkbox"/>	Security settings
<input type="checkbox"/>	Last seen
<input type="checkbox"/>	Grouping of devices

Security	
<input type="checkbox"/>	Remote Lock Unlock Wipe
<input type="checkbox"/>	Specification of PIN/password query and complexity
<input type="checkbox"/>	Identification of firmware manipulations (Jailbreak, Root)
<input type="checkbox"/>	Set guidelines for device encryption
<input type="checkbox"/>	Whitelist blacklist support for apps
<input type="checkbox"/>	Deactivation of system apps

<input type="checkbox"/>	Deactivation of WLAN
<input type="checkbox"/>	Deactivation of Bluetooth
<input type="checkbox"/>	Password History Reset Set new password
<input type="checkbox"/>	Allow / Do not allow access to SD card
<input type="checkbox"/>	Allow / Do not allow access to app stores
<input type="checkbox"/>	WLAN auto-connect

	Compliance
<input type="checkbox"/>	Detect lack of required apps
<input type="checkbox"/>	Detect installation of undesirable apps
<input type="checkbox"/>	Identification of incorrect configuration
<input type="checkbox"/>	Identification of outdated operating system versions
<input type="checkbox"/>	Status and history of rule violations

5 Summary

There isn't one EMM solution that is the right choice for all companies. It is important to define the functional scope precisely and test suitable solutions. In addition to the functionalities offered, the type of operation and handling of the solution also play a crucial role. And it's not just about the technology – the employees also have to be on board, as without their acceptance, the entire mobility project is doomed to failure. For this reason, when choosing an EMM solution, IT managers should always bear in mind the need to strike a fair balance between the security requirements of the company, the employees' acceptance of using mobile devices, and the ease of use of the management options by the administrator. All three points must be considered for a successful introduction of an EMM solution.

About baramundi software AG

baramundi software AG provides companies and organizations with efficient, secure, and cross-platform management of workstation environments. Around the world, over 2,500 customers of all sizes and from every sector benefit from the German manufacturer's many years of experience and outstanding products. These products are combined together in baramundi Management Suite in accordance with an integrated, future-orientated unified endpoint management approach: endpoint management, mobile device management, and endpoint security are provided via a common interface, in a single database, and according to uniform standards.

baramundi Management Suite optimizes IT management processes by automating routine tasks and providing an extensive overview of the status of all endpoints. It relieves the pressure on IT administrators and ensures that wherever users are located, they always have the necessary rights and applications on all platforms and form factors, whether on PCs, notebooks, mobile devices, or in virtual environments.

baramundi software AG is headquartered in Augsburg. The products and services of the company, which was founded in 2000, are fully Made in Germany. baramundi successfully works with partner companies around the world in sales, consultancy, and user support.

More information about baramundi: www.baramundi.com

Would you like to see the EMM solution? Register for the live webcast

See how to manage smartphones and tablets as easily and reliably as PCs and notebooks:
www.baramundi.com/webinar


**We are looking forward
to meeting you!**


Get in touch!





baramundi software AG

Beim Glaspalast 1
86153 Augsburg, Germany

 +49 (821) 5 67 08 - 380
request@baramundi.de
www.baramundi.de

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

 +44 (2071) 93 28 77
request@baramundi.co.uk
www.baramundi.co.uk

 +48 (735) 91 44 54
request@baramundi.pl
www.baramundi.pl


baramundi software Austria GmbH

Landstraßer Hauptstraße 71/2
1030 Wien, Austria

 +43 (1) 7 17 28 - 545
request@baramundi.at
www.baramundi.at

baramundi software USA, Inc.

550 Cochituate Road, Suite 25
Framingham, MA 01701, USA

 +1 (508) 861 75 61
requestUSA@baramundi.com
www.baramundi.com

Empower your IT