baramundi Mobile Devices

The management and protection of mobile devices is an mandatory task for most companies: To simplify corporate processes and to guarantee security, all devices with a variety of mobile operating systems must be managed centrally. Within our solution all popular mobile operating systems - iOS, Android, Windows Mobile and Samsung KNOX - are supported. Moreover your IT administration is relieved by automation of routine tasks and self-service functions.

	Function	Description	Benefit
General	Support for various mobile platforms through unified configuration	Administrators are often asked to support different mobile platforms. Therefore managing all devices through a unified interface is obvious. The EMM solution from baramundi makes a standardised configuration available. In that way the administrator can configure different mobile devices with an unified interface independent of platform.	Less complexity and time saving in configuration of mobile devices Fast results and uninterrupted operation through unified usability
	Automation of database access via API	Provides integration possibilities to external systems through database access via API. Advantages of the new interface are the secure connection via Secure Socket Layer (SSL) and the server side authentication. In addition, there is the possibility of authenticating the clients by login.	Easy integration into third-party systems Creating and updating of data can be easily automated and synchronized via the API
	Mobile support for administrators	With the app "bCenter" baramundi supports the mobility of the administrator. bCenter is an addition to classical baramundi management center. The app supports the administrator quickly accessing basic client information, and allows viewing job status and assigning and starting jobs.	Location-independent access to critical client information and functions
Certificates	Secure distribution of certificates to the mobile devices	SCEP = Simple Certificate Enrollment Protocol = distribute certificates securely from the enterprise CA to mobile devices.	Support for the distribution of certificates accessing Microsoft Exchange using SCEP Increased security (protection) and comfort
Security	Avoid threats by jailbreak and rooting recognition	Through a jailbreak or rooted device the protective functions of the operating system are bypassed. The risk of malware increases. In addition, the administration of an unlocked device is restricted because the protection functions can be bypassed. Therefore, companies should generally prohibit such a modification of the operating system via appropriate policies.	Avoiding real threats Reducing the risk of malicious software
	Ensure a secure app environment on mobile devices	Apple and Google can not provide adequate security controls. Many apps do not meet the minimum security requirements of most companies. Therefore administrators have to create a secure app environment on their mobile devices. Black and whitelisted apps help to protect sensitive business and personal data.	Optimization of internal app auditing Immediate protection of all managed mobile devices Increasing employee awareness and minimize the risk of liability for employees and IT
Configuration	Extensive support of the Apple Volume Purchase Program (VPP)	In addition to supporting the app purchase via VPP Redemption Codes baramundi Mobile Devices also support an alternative app distribution via Managed Distribution Client Assignment. In this way licenses can be bought and assigned for iOS devices instead of having to link licenses to the users Apple IDs.	Administration of apps is facilitated Cost reduction Clarity rises
	Quick & easy integration of new iOS devices in EMM solution (DEP)	Baramundi Mobile Devices support the possibility of allowing immediate enrollment. The administrator can customize this configuration process to his own needs. During the activation process he can define what is the end user allowed to change and what they are not.	Quick and easy activation of the device by end users Improve security issues company-wide Better automation of processes
	App configuration via GUI or XML structure	Baramundi is a member of the AppConfig community. With the aim of simplifying the configuration of apps using native resources of the operating system manufacturers, baramundi Mobile Devices allows these standardized methods and allows easy configuration of compatible apps.	Fast and easy configuration of app settings Use MAM functions to configure and secure mobile devices Use MCM functions (e.g. data synchronization, data processing) of compatible apps
Compliance	Automated compliance management	You need to detect security gaps on the computers in your corporate environment and close them as quickly as possible. Baramundi Mobile Devices shows infringements of company and security rules on mobile devices in a clear Compliance dashboard, from missing apps to jailbreaks. You ensure that devices are configured securely, specify passwords, and remotely delete lost devices.	Clear rules that apply to everyone Clean, cost-efficient licensing Secure configuration Up-to-date systems and a minimized target for malware attacks

More info: baramundi.com/info-mdm

	Function*	iOS	Android	KNOX	Windows
General	Clear interface with filters within bMS	✓	✓	✓	✓
	Integrated Endpoint Management	✓	✓	✓	✓
	Cross-platform configuration	✓	✓	✓	✓
	Role-based access	✓	✓	✓	✓
	Encrypted connection to the MDM interface	✓	✓	✓	✓
	Extensive API	✓	✓	✓	✓
	Mobile administration via app (bCenter)	✓	✗	✗	✗
	MDM - reporting with export possibility	✓	✓	✓	✓
Certificates	Company certificates for MS Exchange (SCEP)	✓	✓	✓	✓
	Company certificates for Enterprise WiFi (SCEP)	✓	✓	✓	✓
	Management of root and intermediate certificates	✓	✓	✓	✓
Enrollment	Enrollment via Intranet | Internet	✓ ✓	✓ ✓	✓ ✓	✓ ✓
	Enrollment via app	✓	✓	✓	✓
	Protection by password / AD authentication	✓ ✓	✓ ✗	✓ ✗	✓ ✓
	Microsoft Active Directory Integration	✓	✗	✗	✓
Security	Remote Lock | Unlock | Wipe	✓ ✓ ✓	✓ N/A ✓	✓ N/A ✓	✓ N/A ✓
	Set PIN/password query and complexity	✓	✓	✓	✓
	Detection of firmware manipulation (jailbreak, root)	✓	✓	✓	N/A
	Set policies for device encryption	N/A	✓	✓	✓
	Support whitelist | blacklist for apps	✓ ✓	N/A N/A	✓ ✓	✓ ✓
	Deactivation of system apps	✓	✗	✓	✓
	Mandatory apps	✓	✓	✓	✓
	Prevent "Copy & Paste"	✗	N/A	✓	✓
	Antivirus integration as app | on server	N/A ✗	✗ ✗	✗ ✗	✗ ✗
	Password history | reset | set new password	✓ ✓ N/A	✓ ✓ ✓	✓ ✓ ✓	✓ ✓ N/A
	Prevent access to SD card	N/A	✗	✓	✓
	Deactivation WiFi	N/A	✗	✓	✓
	Deactivation Bluetooth	N/A	✗	✓	✓
	Prevent wired ActiveSync connections	✓	✗	✗	✓
	Allow/restrict App Store access	✓	N/A	✓	✓
	Allow/restrict YouTube app	✓	✗	✓	✓
	Allow/restrict browser usage	✗	✗	✗	✓
	Restrict e-mail forwarding	✓	✗	✗	✗
	Allow/restrict data connection while roaming	N/A	✗	✗	✓
	Allow/restrict new contacts synchronization	✓	✗	✗	✗
	Allow/restrict Siri | Google NOW | Cortana	✓ N/A N/A	N/A ✗ N/A	N/A ✗ N/A	N/A N/A ✓
	Enforcing SD card encryption	N/A	N/A	✓	N/A
	Protection of settings against modification	✓	✗	✗	✓
	Allow/restrict WiFi auto connect	✓	✗	✗	✓
Inventory	Hardware information	✓	✓	✓	✓
	Configured restrictions (e.g. iCloud lock)	✓	✓	✓	✓
	Installed profiles	✓	✗	✗	✗
	Installed certificates	✓	✓	✓	✓
	SIM information	✓	✓	✓	✓
	Roaming status	✓	✗	✗	✓
	Security settings	✓	✓	✓	✓
	Last contact	✓	✓	✓	✓
	Grouping devices	✓	✓	✓	✓
Configuration	Distribution firmware updates	✓	N/A	N/A	✗
	Installation with | without user confirmation	✓ ✓	✓ N/A	✓ ✗	✓ ✗
	Uninstall with | without user confirmation	N/A ✓	✓ N/A	✓ ✗	N/A N/A
	Installation from App Store	✓	N/A	N/A	✓
	Support Apple Volume Purchase Program (VPP)	✓	N/A	N/A	N/A
	Support Apple Device Enrollment Program (DEP)	✓	N/A	N/A	N/A
	Installation | Uninstall with deactivated App Store	✓ ✓	✓ ✓	✓ ✓	N/A N/A
	Installation | Uninstall of enterprise apps	✓ ✓	✓ ✓	✓ ✓	✓ ✓
	Self-Service app	✓	✓	✓	✓
	Installation | Uninstall certificates	✓ ✓	✓ N/A	✓ ✓	✓ ✓
	Parameterization settings using variables	✓	✓	✓	✓
	App configuration	✓	✗	✗	✗
	Deactivation of the camera	✓	✓	✓	✓
	Configuration of access points	✓	✓	✓	✓
	VPN settings	✓	✓	✓	✗
Compliance	Lack of necessary apps	✓	✓	✓	✓
	Installation of unwanted apps	✓	✓	✓	✓
	Recognition misconfiguration	✓	✓	✓	✓
	Status and history of rule violations	✓	✓	✓	✓

✓ = integrated

✗ = not integrated

N/A = not available

*) Device and configuration-specific restrictions may apply.