CMServices — Mobile Device Management Checklist

Critical Capability	Android		iOS			WinMobile	RIM
	Samsung Galaxy	Motorola Xoom	iPhone	iPad	iPad2	WinMobile	Blackberry
Service Model							
Software As A Service (Vendor Managed)	yes	yes	yes	yes	yes	yes	yes
Hosted (Customer Managed)	yes	yes	yes	yes	yes	yes	yes
Device Hardware Management							
Asset Management	yes	yes	yes	yes	yes	yes	yes
Version Control	yes	yes	yes	yes	yes	yes	yes
Reporting & Alerts	yes	yes	yes	yes	yes	yes	yes
Time Synchronization	no	no	no	no	no	no	no
Provisioning Time	1 Minute	1 Minute	1 Minute	1 Minute	1 Minute	1 Minute	1 Minute
Provision Client via SMS	yes	yes	yes	yes	yes	yes	no
Provision client via SD Card	yes	yes	no	no	no	yes	no
Provision client via APP Store	yes	yes	yes	yes	yes	yes	yes
Provision client via website (URL)	yes	yes	yes	yes	yes	yes	no
Provision client via email	yes	yes	no	no	no	yes	no
Provision client without APP Store	yes	yes	yes	yes	yes	yes	yes
Provision device by group	no	no	no	no	no	no	no
Enable/Disable GPS device	yes	yes	no	no	no	yes	yes
Low CPU Utilization	yes	yes	yes	yes	yes	yes	yes
Device Software Management							
Ability to send software[1]	yes	yes	yes	yes	yes	yes	yes
Synchronize Files Automatically	yes	yes	no	no	no	yes	no
Resumable Downloads	yes	yes	no	no	no	yes	no
Upload large files > 2GB	yes	yes	no	no	no	yes	no
Send large packages > 500 MB	yes	yes	no	no	no	yes	no
Self service	yes	yes	yes	yes	yes	yes	yes
Prevent Uninstall of APPs by user	no	no	no	no	no	no	yes
Enable/Disable Enterprise APPs	yes	yes	yes	yes	yes	yes	yes
Package Scheduling	yes	yes	yes	yes	yes	yes	yes
Software version control	yes	yes	yes	yes	yes	yes	yes
Windows Application Updates	n/a	n/a	n/a	n/a	n/a	yes	n/a
Backup and Recovery[2]	yes*	yes*	no	no	no	yes*	no
Software inventory	yes	yes	yes	yes	yes	yes	yes
Collect iOS UDID info	n/a	n/a	yes	yes	yes	n/a	n/a
Enterprise APP Store	yes	yes	yes	yes	yes	yes	yes
Firmware Software Upgrades[3]	no	no	no	no	no	no	yes
File compression	no	no	no	no	no	no	no
Bit-level syncing	no	no	no	no	no	no	no
Block/Allow Access to Corp email	yes	yes	yes	yes	yes	yes	yes
Patch packaging and relevance	yes	yes	yes	yes	yes	yes	yes
Network Access Control							
VPN Block	no	no	no	no	no	no	yes
VPN Teardown	no	no	no	no	no	no	no
Network Restrict[7]	yes	yes	yes	yes	yes	yes	yes*
Black List / White List URLs (proxy)	no	no	no	no	no	no	no
VPN Enforcement	yes	yes	yes	yes	yes	yes	yes
Messaging							
Send message to one device	yes	yes	yes	yes	yes	yes	yes
Send message to multiple devices	yes	yes	yes	yes	yes	yes	yes
Pull data from a device on demand for reporting	yes	yes	yes	yes	yes	yes	yes
Remote Control							
Remote Control[8]	yes*	yes*	no	no	no	yes	yes
Remote Control two-way chat	yes	yes	no	no	no	yes	no
Remote File Send/Receive	yes	yes	no	no	no	yes	no
Process/Application Manager	yes	yes	no	no	no	yes	no
Remote Registry View/Update	n/a	n/a	n/a	n/a	n/a	yes	n/a
Remote Recording[9]	yes*	yes*	no	no	no	yes	yes*
Remote Reset	yes	yes	yes	yes	yes	yes	yes
GPS Locate							
GPS Tracking	yes	yes	yes	yes	yes	yes	yes
Bread Crumbs	no	no	no	no	no	no	no
Speed Alerts	no	no	no	no	no	no	no
Geo Fences/Zones[15]	Yes*	Yes*	no	no	no	no	no

CMServices
Mobile Device Management Checklist

Critical Capability	Android Samsung Galaxy	Android Motorola Xoom	iOS iPhone	iOS iPad	iOS iPad2	WinMobile	RIM Blackberry
Security							
KIOSK Mode	yes	yes	yes	yes	yes	yes	yes
Manage Encryption on Hard Disk[10]	yes*	yes*	yes	yes	yes	yes	yes
Enforce A/V use windows updates	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Auth Proxy Support	no	no	yes	yes	yes	no	no
Communications over SSL	yes	yes	yes	yes	yes	yes	yes
Lock/Unlock Device	yes	yes	yes	yes	yes	yes	yes
Force Use of Passcode	yes	yes	yes	yes	yes	yes	yes
Wipe Device	yes	yes	yes	yes	yes	yes	yes
Wipe SD Card	yes	yes	yes	yes	yes	yes	yes
Selective Wipe Device (email)[11]	yes*	yes*	yes	yes	yes	yes	yes
Selective Wipe Device (files)[12]	yes*	yes*	yes	yes	yes	yes*	no
Locate (via cell tower)	no	no	no	no	no	no	no
Locate (via GPS)	yes	yes	no	no	no	yes	yes
Password Policy	yes	yes	yes	yes	yes	yes	yes
Certificate Distribution	yes	yes	yes	yes	yes	yes	no
White List/Black List APPs	yes	yes	yes	yes	yes	yes	no
ActiveSync Policy	yes	yes	yes	yes	yes	yes	n/a
Block Registration by OS	yes	yes	yes	yes	yes	yes	n/a
Restrict/Block Access to APP Store	no	no	yes	yes	yes	no	yes
Restrict SMS	no	no	no	no	no	no	yes
Jailbreak/Root Detection	yes	yes	yes	yes	yes	yes	n/a
Active Directory Policy Support	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Out Of Contact Policy	yes	yes	yes	yes	yes	yes	no
Role Based Administration	yes	yes	yes	yes	yes	yes	yes
Encrypted data transport[13]	yes*	yes	yes	yes	yes	yes	yes
Auditing	yes	yes	yes	yes	yes	yes	yes
Remote backup[14]	yes*	yes*	no	no	no	yes*	no
Trust/Untrust Wi-Fi	no	no	yes	yes	yes	no	yes
Reporting							
Enterprise Global Reporting	yes	yes	yes	yes	yes	yes	yes
Anti-Virus Reporting[4]	yes	yes	yes	yes	yes	yes	yes
OS Patch Management	no	no	no	no	no	no	no
Global Software Inventory	yes	yes	yes	yes	yes	yes	yes
Compliance Reporting	yes	yes	yes	yes	yes	yes	yes
Policy Enforcement	yes	yes	yes	yes	yes	yes	yes
Filtering and Grouping of devices	yes	yes	yes	yes	yes	yes	yes
Supports a custom reporting platform	yes	yes	yes	yes	yes	yes	yes
Graphical Reporting	yes	yes	yes	yes	yes	yes	yes
Connectivity Reporting (3G, Wi-Fi, Ethernet)	no	no	no	no	no	no	no
Connectivity Security Method[5]	HTTPS/SSL	HTTPS/SSL	HTTPS/SSL	HTTPS/SSL	HTTPS/SSL	HTTPS/SSL	HTTPS/SSL
Track status of multiple independent packages	yes	yes	yes	yes	yes	yes	yes
Report on device statistics	yes	yes	yes	yes	yes	yes	yes
Report on data usage[6]	yes*	yes*	no	no	no	yes*	no
Alerts	yes	yes	yes	yes	yes	yes	yes

1iOS is a install link push. User clicks link to install software.

2CMServices can manually backup file systems on Android and Windows Mobile platforms. This could be further automated via our Dynamic Defense capability, but is not out of the box.

3BlackBerry device firmware can be pushed from the BES.

4Via application lists blacklists.

5All communication between the Server(s), devices and consoles is encrypted using HTTPS/SSL.

6CMServices can track data transmitted through application tunnels.

7Yes via BES Policy.

8CMServices can remote control (i.e., similar to remote desktop for PCs) Windows Mobile, BlackBerry and Andro id devices. Android devices must be rooted in order perform the function of controlling the device.

9Recording and screen capture are dependent on Carrier and phone manufacturer. Some device screen capture requires no elevated permissions, while others require root access to be able to remotely view the screen.

10Yes via NitroDesk TouchDown.

11Yes via NitroDesk TouchDown.

12Yes via Remote Support console.

13Android Pre 3.0 devices do not have encryption capabilities. CMServices provides email encryption on these devic es via TouchDown.

14CMServices can manually backup file systems on Android and Windows Mobile platforms. This could be further autom ated via our Dynamic Defense capability, but is not out of the box.

15Geo Fencing can be done via Dynamic Defense Professional Services.