

So richten Sie iOS-Geräte mit Cortado MDM BSI-konform ein

Umsetzungshilfe zu den IT-Grundschutz-Bausteinen des BSI

White Paper



Inhalt

Hintergrund	3
Umsetzung der BSI-Anforderungen	4
Basis-Anforderungen und Benutzergruppen.....	4
Passwort-Richtlinien	5
OS-Update-Richtlinien	7
Richtlinien zur Nutzung von Gerätefunktionen	7
Richtlinien für Supervised Devices	13
Fazit	15

Hintergrund

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Umsetzungshinweise für iOS-Geräte in Unternehmen ausgegeben¹. Als die nationale Cyber-Sicherheitsbehörde in Deutschland gestaltet das BSI „Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft“². Das Modul „SYS.3.2.3 iOS (for Enterprise)“ ist Bestandteil des umfassenden IT-Grundschutz-Kompends. Es enthält grundlegende Anforderungen für den Betrieb von iOS-basierten Geräten, welche in den Workflow einer Institution integriert sind.

In Behörden gibt es häufig Vorgaben, die gesamte IT-Architektur BSI-konform einzurichten. Allein aufgrund der Autorität des Amtes im Bereich IT-Sicherheit ist das auch für Unternehmen und Organisationen empfehlenswert. Denn das Kernproblem bleibt für alle gleich: Apples iOS, das laut verschiedenen Umfragen auf den meisten mobilen Geräten in der Geschäftswelt zu finden ist³, wird vorrangig für den persönlichen Gebrauch entwickelt. iPhones und iPads im Unternehmenseinsatz bergen deshalb diverse Sicherheitsrisiken. Zum Beispiel können via iOS-Geräte sensible Daten verloren gehen oder schädliche Software in das Unternehmensnetzwerk gelangen.

Gleichzeitig ist jedoch klar, dass mobile Geräte nicht vom Arbeitsplatz verbannt werden können oder sollten. Smartphones und Tablets vereinfachen den Zugriff auf digitale Informationen. Angesichts zunehmender mobiler Arbeitsweisen wird der Fernzugriff auf Unternehmensserver durch mobile Geräte zukünftig auch schwer zu vermeiden sein. Laut einer StepStone-Studie arbeiten 15% der Befragten an wechselnden Standorten⁴. Andere Studien haben festgestellt, dass im Jahr 2040 „mobiles Arbeiten zur neuen Norm wird“⁵. Zudem sind auf iOS-Geräten zahlreiche Produktivitäts-Tools und AR-Apps vorinstalliert, und jeden Tag werden neue Applikationen entwickelt und veröffentlicht. Dank MDM-Lösungen wird die Bereitstellung von mobilen Geräten sowie deren Konfiguration immer komfortabler für die IT-Abteilungen.

Es ist unbestritten, dass der Einsatz von iOS-Geräten für Unternehmen, Institutionen und Behörden von großem Nutzen sein kann⁶. Richten Sie Ihre mobilen Geräte an den BSI-Richtlinien aus, dann können Sie die Vorteile ausschöpfen und gleichzeitig Ihr Unternehmen weniger anfällig für IT-Sicherheitsverletzungen oder Datenverlust machen.

In diesem White Paper zeigen wir Ihnen die vom BSI empfohlenen Richtlinien und wie Sie mit Cortado MDM im Unternehmen eingesetzte iOS-Endgeräte konform zu den BSI-Hinweisen konfigurieren können.

1 Den vollständigen BSI-Artikel finden Sie [hier](#). Darüber hinaus können Sie das komplette **IT-Grundschutz-Kompensum 2019** einsehen.

2 https://www.bsi.bund.de/DE/DasBSI/Leitbild/leitbild_node.html. (Abgerufen Mai 2019)

3 Siehe z.B. „iOS im Unternehmen: Steigende Nutzerzahlen und beliebter als Android“. (2018) <https://www.macwelt.de/a/ios-im-unternehmen-steigende-nutzerzahlen-und-beliebter-als-android,3439609>. Auch „Apple iOS versus Google Android im Unternehmenseinsatz“. <https://www.computerweekly.com/de/feature/Apple-iOS-versus-Google-Android-im-Unternehmenseinsatz>. (Abgerufen Mai 2019)

4 StepStone Mobilitäts-Report (2018) https://www.stepstone.de/Ueber-StepStone/wp-content/uploads/2018/04/StepStone_Mobilit%C3%A4tsreport_2018-1.pdf. (Abgerufen Mai 2019)

5 Die Evolution der Mobilität (2017) https://www.zukunftsinstitut.de/fileadmin/user_upload/Publikationen/Auftragsstudien/ADAC_Mobilitaet2040_Zukunftsinstitut.pdf. S. 10, S.12 (Abgerufen Mai 2019)

6 <https://www.bechtle.com/marken/apple/ios-in-business>. (Abgerufen Mai 2019)

Umsetzung der BSI-Anforderungen

Basis-Anforderungen und Benutzergruppen

Das BSI legt grundlegende Anforderungen fest, die jedes Unternehmen erfüllen sollte. Grundvoraussetzung hierfür ist der Einsatz einer kompatiblen Mobile-Device-Management-Lösung wie Cortado MDM. Darüber hinaus benötigen Sie eine Strategie für die iOS-Nutzung, einen Plan für die Nutzung von Cloud-Diensten und Maßnahmen gegen das unbefugte Löschen von Konfigurationsprofilen.

Das BSI gliedert Nutzer in drei fiktive Nutzergruppen, um die unterschiedlichen Anwendungsfälle und Rahmenbedingungen zu berücksichtigen: Wir zeigen Ihnen anhand dieser drei Beispielgruppen, wie Sie die Umsetzungshinweise vom BSI mit Cortado MDM realisieren können.

- **Benutzergruppe 1:** Diese Benutzergruppe verwendet nur Grundfunktionen des Telefons, hat keinen Dateizugriff und arbeitet nicht mit als vertraulich klassifizierten Datensätzen.
- **Benutzergruppe 2:** Diese Benutzer arbeiten mit Emails auf dem Smartphone, haben Dateizugriff und arbeiten teilweise mit sensiblen Informationen.
- **Benutzergruppe 3:** Diese Benutzer arbeiten mit Emails auf dem Smartphone, haben Zugriff auf Datei-Verzeichnisse und schützenswerte Infrastrukturressourcen. Außerdem arbeiten Sie mit sensiblen und geschäftskritischen Daten.

Das BSI gibt sinnvolle Tipps zum Life Cycle Management von iOS-Geräten, die Sie sich ebenfalls im Originalartikel durchlesen sollten. Wir beschränken uns hier auf Optionen, die Sie mit Cortado MDM gleich umsetzen können. Damit Sie die vollständige Umsetzung der Hinweise überprüfen können, haben wir die jeweiligen Hinweise des BSIs in den Tabellen referenziert.

So richten Sie iOS-Geräte mit Cortado MDM BSI-konform ein

Passwort-Richtlinien

Eine einfache und wirkungsvolle erste Maßnahme ist das Erzwingen eines ausreichend komplexen Gerätecodes. In der Cortado MDM-Konsole können Sie über „Control Panel“ > Policies > „+“ > „iOS Policies“ den Reiter „Password“ auswählen und den Gerätecode konfigurieren, indem Sie „Force Password“ aktivieren (Abb. 1).

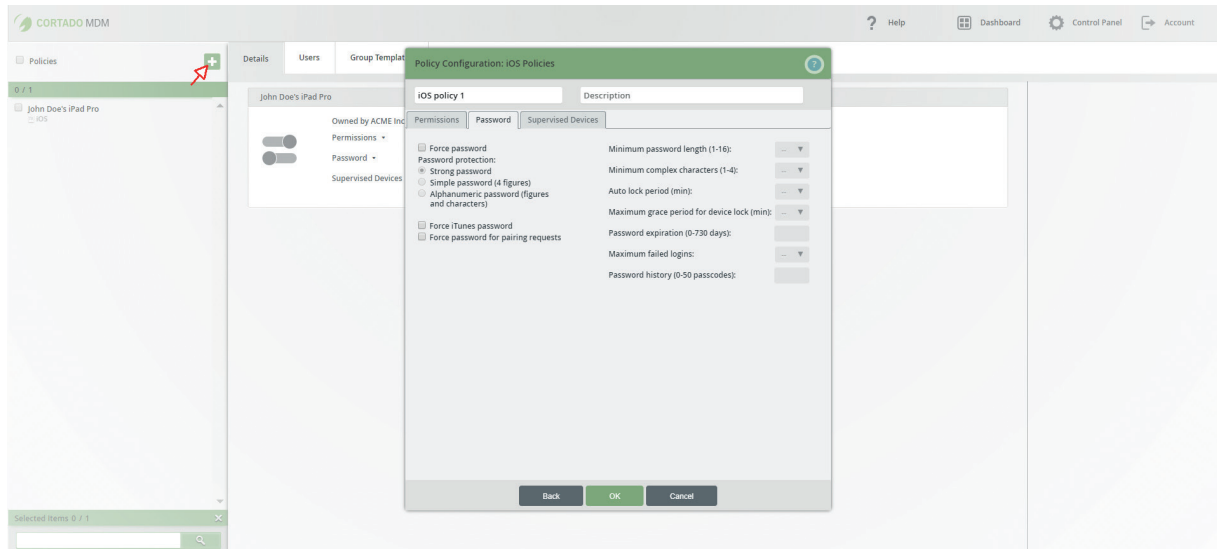


Abb.1: In der Cortado MDM-Konsole können Sie über „Control Panel“ > Policies > „+“ > „iOS Policies“ den Reiter „Password“ auswählen

Hier sind die von dem BSI geschlagenen Einstellungen, welche wir für Sie in unsere Einstellungen übersetzt haben.

BSI-Referenz	Name der Richtlinie – BSI	Name der Richtlinie – Cortado MDM	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
SYS.3.2.3.M9	Einfache Werte erlauben*	Alphanumeric password*	nein	ja	ja
SYS.3.2.3.M3	Mindestlänge des Passcodes	Minimum password length	6	8	8
SYS.3.2.3.M9	Sonderzeichen erforderlich	Minimum complex characters	-	-	1

So richten Sie iOS-Geräte mit Cortado MDM BSI-konform ein

BSI-Referenz	Name der Richtlinie – BSI	Name der Richtlinie – Cortado MDM	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
SYS.3.2.3.M3	Maximale Passcode-gültigkeit	Password expiration	120	90	90
SYS.3.2.3.M4	Automatische Sperre (maximal)	Auto lock period	5	3	2
SYS.3.2.3.M5	Maximale Zeitrenze für Geräte-sperrung	Maximum grace period	1	-	-
SYS.3.2.3.M6	Maximale Anzahl an Fehlversuchen	Maximum failed logins	8	6	3
SYS.3.2.3.M17	Passcode-Verlauf	Password history	5	10	10
SYS.3.2.3.M3	Änderung des Codes erlauben	Passcode modification	ja	ja	ja

*Das BSI empfiehlt, für keine Benutzergruppe einfache PINs zu erlauben. Wir haben uns deshalb entschieden, gleich alphanumerische Passwörter zu empfehlen.

So richten Sie iOS-Geräte mit Cortado MDM BSI-konform ein

OS-Update-Richtlinien

Das BSI empfiehlt, iOS-Updates immer zeitnah zu testen und im Anschluss auf alle Benutzer auszurollen. Die folgende Tabelle enthält die Zeiträume, in welchen ein Update über das MDM forciert werden sollte.

BSI-Referenz	Name der Richtlinie – BSI	Name der Richtlinie – Cortado MDM	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
SYS.3.2.3.M8	Aktualisierungszeitraum (Tage)	Force automatic OS updates	14 Tage	7 Tage	7 Tage
SYS.3.2.3.M8	Unterstützende technische Maßnahmen	NA	Zusätzliche organisatorische Maßnahmen planen. Cortado Reporting verwenden, um Altgeräte, die nicht mehr aktualisiert werden können, zu identifizieren und ggf. auszusortieren.		

Richtlinien zur Nutzung von Gerätefunktionen

Mit weiteren Richtlinien für die Nutzung einzelner Gerätefunktionen kann das Schutzniveau weiter angehoben werden. Wählen Sie unter „Policy Configuration“ den Tab „Permissions“ (Abb. 2) und definieren Sie die Werte je nach Benutzergruppe wie folgt.

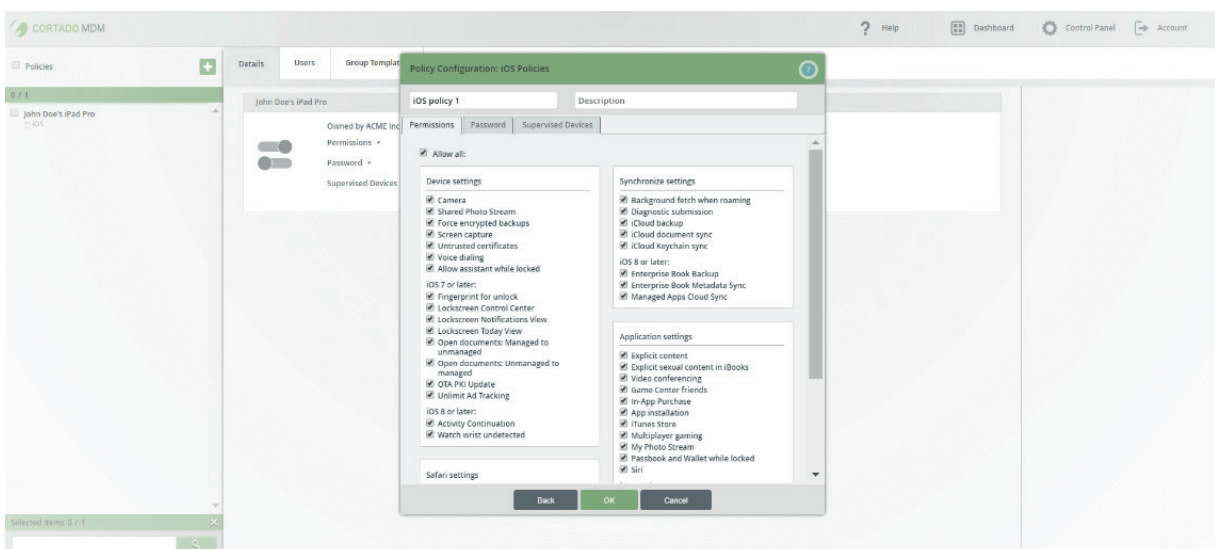


Abb. 2: In der Cortado MDM-Konsole können Sie über „Control Panel“ > Policies > „+“ > „iOS Policies“ den Reiter „Permissions“ auswählen

So richten Sie iOS-Geräte mit Cortado MDM BSI-konform ein

BSI-Referenz	Name der Richtlinie – BSI	Name der Richtlinie – Cortado MDM	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
SYS.3.2.3.M10	Touch-ID zum Entsperren	Fingerprint for unlock	ja	ja	nein
SYS.3.2.3.M10	Touch-ID verwenden für iTunes und App Store	Autofill without authentication	nein	nein	nein
SYS.3.2.3.M10	Ändern der Touch-ID-Fingerabdrücke erlauben	Disallow Fingerprint Modification	nein	ja	ja
SYS.3.2.3.M13	Wallet-Mitteilungen im Sperrbildschirm anzeigen	Passbook and Wallet while locked	ja	ja	nein
SYS.3.2.3.M13	Kontrollzentrum im Sperrbildschirm anzeigen	Lockscreen Control Center	ja	ja	nein
SYS.3.2.3.M13	Mitteilungszentrale im Sperrbildschirm anzeigen	Lockscreen Notifications View	ja	nein	nein
SYS.3.2.3.M13	Ansicht "heute" im Sperrbildschirm anzeigen	Lockscreen Today View	ja	nein	nein
SYS.3.2.3.M13	Siri erlauben	Siri	ja	ja	nein

So richten Sie iOS-Geräte mit Cortado MDM BSI-konform ein

BSI-Referenz	Name der Richtlinie – BSI	Name der Richtlinie – Cortado MDM	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
SYS.3.2.3.M13	Siri erlauben, während das Gerät gesperrt ist	Allow Assistant while locked	nein	nein	nein
SYS.3.2.3.M13	Siri-Obszönitätenfilter aktivieren	Siri Profanity unfiltered	nein	nein	nein
SYS.3.2.3.M13	Benutzergenerierten Inhalt in Siri erlauben	User-generated content in Siri	ja	nein	nein
SYS.3.2.3.M13	FaceTime erlauben	Video conferencing	ja	ja	nein
SYS.3.2.3.M13	iMessage erlauben	iMessage	ja	ja	nein
SYS.3.2.3.M13	Diagnose- und Nutzungsdaten an Apple senden	Diagnostic Submission	nein	nein	nein
SYS.3.2.3.M13	Bildschirmfoto oder Bildschirmaufnahme erlauben	Screen Capture	ja	nein	nein
SYS.3.2.3.M13	Sprachwahl erlauben, während das Gerät gesperrt ist	Voice Dialing	ja	nein	nein
SYS.3.2.3.M13	Backup unternehmenseigener Bücher erlauben	Enterprise Book Backup	nein	ja	ja

So richten Sie iOS-Geräte mit Cortado MDM BSI-konform ein

BSI-Referenz	Name der Richtlinie – BSI	Name der Richtlinie – Cortado MDM	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
SYS.3.2.3.M13	Verschlüsselte Backups erzwingen	Force Encrypted Backups	ja	ja	ja
SYS.3.2.3.M13	Beschränktes Ad-Tracking erzwingen	Unlimit Ad Tracking	nein	nein	nein
SYS.3.2.3.M13	Benutzer dürfen nicht vertrauenswürdige TLS-Zertifikate annehmen	Untrusted Certificates	ja	nein	nein
SYS.3.2.3.M13	Einstufen neuer Entwickler firmeneigener Apps als vertrauenswürdig erlauben	Enterprise App Trust	ja	nein	nein
SYS.3.2.3.M13	Änderung der Beschränkungen erlauben	Enabling Restrictions	ja	ja	ja
SYS.3.2.3.M13	Automatische Updates für Trust-Zertifikate erlauben	OTA PKI Update	ja	ja	ja
SYS.3.2.3.M13	Dokumente von verwalteten Quellen in nicht verwalteten Zielen erlauben	Open Documents: Managed to Unmanaged	ja	nein	nein

So richten Sie iOS-Geräte mit Cortado MDM BSI-konform ein

BSI-Referenz	Name der Richtlinie – BSI	Name der Richtlinie – Cortado MDM	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
SYS.3.2.3.M13	Dokumente von nicht verwalteten Quellen in verwalteten Zielen erlauben	Open Documents: Unmanaged to Managed	ja	nein	nein
SYS.3.2.3.M14	iCloud Backup erlauben	iCloud backup	ja	nein	nein
SYS.3.2.3.M14	iCloud-Dokumente und -Daten erlauben	iCloud document Sync	ja	nein	nein
SYS.3.2.3.M14	iCloud Schlüsselbund erlauben	iCloud keychain sync	nein	nein	nein
SYS.3.2.3.M14	Verwalteten Apps das Sichern von Daten in iCloud erlauben	Managed Apps iCloud Sync	ja	nein	nein
SYS.3.2.3.M14	Synchronisieren von Notizen und Anmerkungen für unternehmenseigene Bücher erlauben	Enterprise Book Metadata Sync	ja	ja	nein
SYS.3.2.3.M15	AirDrop als nicht verwalteten Zielort behandeln	AirDrop unmanaged	ja	nein	nein
SYS.3.2.3.M15	Handoff erlauben	Activity Continuation	ja	nein	nein

So richten Sie iOS-Geräte mit Cortado MDM BSI-konform ein

BSI-Referenz	Name der Richtlinie – BSI	Name der Richtlinie – Cortado MDM	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
SYS.3.2.3.M16	Code-Eingabe bei erster AirPlay-Verbindung anfordern	Force Password for pairing requests	ja	ja	ja
SYS.3.2.3.M18	Automatisches Ausfüllen aktivieren	AutoFill	ja	nein	nein
SYS.3.2.3.M18	Betrugswarnung erzwingen	Hide fraudulent website warning	nein	nein	nein
SYS.3.2.3.M18	Popups unterdrücken	Popups	ja	nein	nein
SYS.3.2.3.M18	Cookies akzeptieren	Allow Cookies	always	From visited sites	From visited sites

So richten Sie iOS-Geräte mit Cortado MDM BSI-konform ein

Richtlinien für Supervised Devices

Kommen im Unternehmen betreute iPhones und/oder iPads zum Einsatz, sind die folgenden Einstellungen empfehlenswert. In der Cortado MDM-Konsole können Sie diese unter „Policy Configuration“ im Tab „Supervised Devices“ vornehmen (Abb. 3).

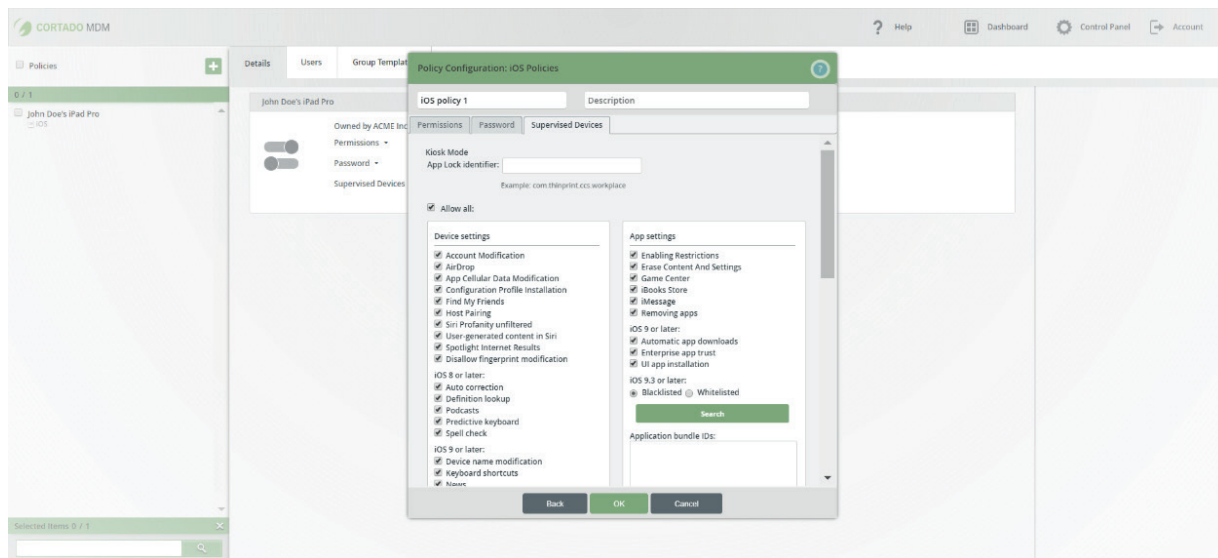


Abb. 3: In der Cortado MDM-Konsole können Sie über „Control Panel“ > Policies > „+“ > „iOS Policies“ den Reiter „Supervised Devices“ auswählen

BSI-Referenz	Name der Richtlinie – BSI	Name der Richtlinie – Cortado MDM	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
SYS.3.2.3.M11	Ändern des Gerätenamens erlauben	Device name modification	nein	nein	nein
SYS.3.2.3.M13	Ändern des Hintergrundbilds erlauben	Wallpaper Modification	ja	ja	nein
SYS.3.2.3.M13	Ändern der Diagnose und Nutzerdatenübermittlungseinstellung erlauben	Diagnostics submission modification	nein	nein	nein

So richten Sie iOS-Geräte mit Cortado MDM BSI-konform ein

BSI-Referenz	Name der Richtlinie – BSI	Name der Richtlinie – Cortado MDM	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
SYS.3.2.3.M13	Löschen aller Inhalte erlauben	Erase content and Settings	ja	ja	nein
SYS.3.2.3.M14	Ändern der Einstellungen von “Freunde suchen” erlauben	Find My Friends	nein	nein	nein
SYS.3.2.3.M15	AirDrop erlauben	AirDrop	ja	ja	nein
SYS.3.2.3.M21	Installation von Apps über den App Store erlauben	UI App Installation	ja	ja	nein
SYS.3.2.3.M21	Automatische App-Downloads erlauben	Automatic app downloads	ja	nein	nein
SYS.3.2.3.M21	Entfernen von Apps erlauben	Remove Apps	ja	ja	nein
SYS.3.2.3.M21	In-App-Käufe erlauben	In-App Purchase	ja	ja	nein



Fazit

Mit den oben genannten Richtlinien und Vorschlägen des BSI können Sie mit Cortado MDM im Unternehmen eingesetzte iOS-Geräte besser absichern. Zusätzlich zu den Richtlinien schlägt das BSI vor, Filteroptionen, HTTP Proxies und VPN zu verwenden. Es können hier allerdings keine generellen Empfehlungen ausgesprochen werden, da diese sehr von Ihrem Anwendungsfall abhängig sind.

Wenn Sie mehr über diese Möglichkeiten wissen möchten, weiterführende Fragen haben, oder Ihre Endnutzer nicht in die vom BSI vorgeschlagenen Kategorien einordnen können und unseren Rat möchten, dann kontaktieren Sie uns gerne, damit wir Optionen miteinander absprechen können.

..... Headquarters

Cortado Mobile Solutions GmbH

Alt-Moabit 91a/b
10559 Berlin, Germany
Tel.: +49 (0)30 408 198 500
Fax: +49 (0)30 408 198 501
E-Mail: info@cortado.de
www.cortado.de

Cortado Pty Ltd.

..... Australia

Level 12, Plaza Building,
Australia Square, 95 Pitt Street
NSW 2000 Sydney, Australia
Tel.: +61-(0)2-8079 2989

..... USA (Colorado)

Cortado, Inc.

3858 Walnut Street, Suite 130
Denver, CO 80205, USA
Tel.: +1-303-487-1302
E-mail: info@cortado.com
www.cortado.com

Cortado Japan

..... Japan

5F Yaesu Dori Building,
3-4-15 Nihonbashi,
Chuo-ku Tokyo
Tokyo 103-0027
Tel.: +81-(0)3-6870 3467



Alle Namen und Warenzeichen sind Namen und Warenzeichen der jeweiligen Hersteller.

Folgen Sie Cortado auf:



facebook



twitter



youtube



linkedin