Konfigurationsempfehlungen für Jamf School

In Jamf School sind eine Vielzahl von Konfigurationsoptionen umgesetzt. Viele haben keinerlei Auswirkungen auf die datenschutzkonforme Konfiguration oder sind in Abhängigkeit von übergeordneten Einstellungen aktiviert oder deaktiviert.

Sie finden in der Tabelle empfohlene Einstellungsoptionen, die den unterschiedlichen Schutzniveaustufen für dienstliche iPads zugeordnet sind.

Legende

Farbcode	Bedeutung
	Haken setzen
	Haken nicht setzen
	Haken setzen nach begründeter Abwägung möglich - bei Unsicherheit Haken nicht setzen
	nicht relevant für iPad / Geräte ohne LTE
	unklar, ob (im Notfall) technisch erforderlich

Für die technische und formale Korrektheit der Empfehlungen wird kein Gewähr gegeben!

Payload Code

Gerätefunktionen	Schutzstufe D
Einfache Werte erlauben	
Alphanumerische Werte erforderlich	
Mindestlänge des Codes	8 Zeichen
Mindestanzahl von komplexen Zeichen	2 Zeichen
Maximale Code-Gültigkeit (in Tagen)	1 Jahr
Automatische Sperre (max.) (in Minuten)	1 Minuten
Code-Verlauf	3
Maximale Zeitgrenze für Gerätesperrung	sofort
Maximale Anzahl von Fehlversuchen	3

Payload Einschränkungen

Gerätefunktionen	Schutzstufe D	Kommentar
Verwenden der Kamera erlauben		
Sprachwahl erlauben		
FaceTime erlauben		
Bildschirmaufnahmen erlauben		
Bildschirmbeobachtung über Classroom erlauben		
Automatisches Synchronisieren beim Roaming erlauben		
Installation von Apps erlauben		

Entfernen von Apps erlauben		
In-App-Käufe erlauben		
Siri erlauben		
Siri bei gesperrtem Gerät erlauben		
Benutzergenerierte Inhalte Siri erlauben		
Siri Filter für anstößige Sprache aktivieren		
Serverseitige Protokollierung für Siri erlauben		
Einschränkungen/Bildschirmzeit erlauben		
Fortsetzen von Aktivitäten (Handoff) erlauben		
Nachschlagen im Wörterbuch erlauben		
QuickType Textvorschläge erlauben		
Auto-Korrektur erlauben		
Rechtschreibprüfung erlauben		
AirDrop erlauben		
AirDrop als nicht verwaltetes Ziel behandeln		
Spotlight Vorschläge erlauben		
Diktierfunktion erlauben		
Diktieren mit Siri verhindern		
Koppeln mit anderen Computern erlauben		Backups sonst nicht möglich!
Modus für eingeschränkten Zugriff über USB erlauben		
Zugriff auf USB-Laufwerke in Dateien App erlauben		
Nahfeldkommunikation (NFC) zulassen		
Sperrbildschirm	Schutzstufe D	Kommentar
Kontrollzentrum auf Sperrbildschirm anzeigen		
Mitteilungszentrale auf Sperrbildschirm anzeigen		
Ansicht „Heute“ auf Sperrbildschirm anzeigen		
Passbook Mitteilungen auf Sperrbildschirm anzeigen		
Anwendungen	Schutzstufe D	Kommentar
Verwenden des iTunes Store erlauben		
Verwenden von Safari erlauben		
Automatisches Einfügen aktivieren		
JavaScript aktivieren		
Deaktivieren des Pop-Up-Blockers durch Benutzer erlauben		
Betrugswarnung erzwingen		
Cookies akzeptieren		
Automatische App-Downloads erlauben		
iMessage erlauben		
Synchronisieren von Notizen und Hervorhebungen in unternehmenseigenen Büchern erlauben		
Podcasts erlauben		
„Mein Gerät suchen“ in der Suche-App erlauben		
„Meine Freunde suchen“ in der Suche-App erlauben		
Game Center erlauben		
Hinzufügen von Freunden im Game Center erlauben		
Multiplayer-Spiele erlauben		
Book Store erlauben		
Apple Music erlauben		

Apple Music Radio erlauben		
Apple News erlauben		
Entfernen von System-Apps erlauben		
Einstufen neuer Entwickler unternehmenseigener Apps als vertrauenswürdig erlauben		
Schreiben von Kontaktdaten in Kontakte nicht verwalteter Accounts durch verwaltete Apps erlauben		
Lesen von Kontaktdaten in Kontakten nicht verwalteter Accounts durch verwaltete Apps erlauben		
Software-Updates zurückstellen für	(15)	
iCloud	Schutzstufe D	Kommentar
Sichern in iCloud erlauben		
iCloud Dokumente und Daten erlauben		
iCloud Schlüsselbund erlauben		
iCloud Fotomediathek erlauben		
Synchronisieren verwalteter Apps mit iCloud erlauben		
Fotostream erlauben		
Gemeinsamen Fotostream erlauben		
Sperrbildschirm	Schutzstufe D	Kommentar
Touch ID das Entsperren des Geräts erlauben		
Senden von Diagnosedaten an Apple erlauben		
Ändern der Diagnoseeinstellungen erlauben		
Dokumente aus verwalteten Apps in nicht verwalteten Apps erlauben		
Dokumente aus nicht verwalteten Apps in verwalteten Apps erlauben		
Verschlüsselte Sicherungen erzwingen		
Beschränktes Ad-Tracking erzwingen		
Eingabe eines iTunes Store Passworts für alle Einkäufe durch den Benutzer durchsetzen		
Verwendung eines Passworts beim Erhalt von AirPlay Kopplungsanfragen von diesem Gerät auf anderen Geräten durchsetzen		
Ändern des Codes erlauben		
Ändern von Touch ID Fingerabdrücken / Face ID Gesichtern erlauben		
Automatisches Einfügen von Passwörtern erlauben		
Vor automatischem Einfügen Authentifizierung erforderlich		
Abfrage von Passwörtern auf Geräten in der Nähe erlauben		
Passwortfreigabe über AirDrop erlauben		
Nicht vertrauenswürdige TLS-Verbindungen mit Bestätigung erlauben		
Interessenbezogene Werbung von Apple erlauben		
Sichern unternehmenseigener Bücher erlauben		
Automatische Updates von Einstellungen für vertrauenswürdige Zertifikate erlauben		
Starten von Geräten im Wiederherstellungsmodus mit einem nicht gekoppelten Gerät, das über ein Lightning Kabel angeschlossen ist, erlauben	Prüfung!	
Autonomer Einzel-App-Modus	Schutzstufe D	Kommentar
Kein Eintrag erforderlich!		
Airprint	Schutzstufe D	Kommentar
AirPrint erlauben		
Speichern der Anmeldedaten für AirPrint im Schlüsselbund erlauben		

Vertrauenswürdiges Zertifikat für TLS-Verbindung mit Druckern erzwingen		
Suche nach AirPrint Druckern per iBeacon erlauben		
Klassenzimmer	Schutzstufe D	Kommentar
Classroom erlauben, für vom Administrator erstellte Klassen für iOS 10 oder älter „Bildschirm anzeigen“ ohne Nachfrage auszuführen		
Beschränken auf App und Sperren des Geräts in Classroom ohne Bestätigung erlauben		
Classroom Klassen ohne Bestätigung automatisch beitreten		
Bei einer von einer Lehrkraft in der Classroom App von Apple erstellten Klasse das Verlassen der Klasse ohne die Erlaubnis der Lehrkraft verhindern		
Verbindung	Schutzstufe D	Kommentar
Koppeln mit Apple Watch erlauben		
Handgelenkerkennung bei Apple Watch erzwingen		
Ändern von Bluetooth-Einstellungen (einschließlich Kopplung neuer Geräte) erlauben		
Geräten nur den Beitritt zu WLAN-Netzwerken erlauben, die mit einem Profil konfiguriert wurden		
WLAN durchgehend aktiviert lassen		
Erstellen von VPN-Konfigurationen erlauben		
Benutzeranpassungen	Schutzstufe D	Kommentar
Ändern der Accounteinstellungen (E-Mail. Kontakte, Kalender, iCloud und iTunes Store)		
Verwenden der Einstellung „Alle Inhalte & Einstellungen löschen“ erlauben		
Ändern der Einstellungen für „Freunde suchen“ erlauben		
Installation von Konfigurationsprofilen erlauben		
Ändern des Gerätenamens erlauben		
Tastaturkurzbefehle erlauben		
App-Installation über den App Store erlauben		
Ändern persönlicher Hotspots erlauben		
Benutzer das Ändern des Hintergrundbilds erlauben		
Ändern von Mitteilungseinstellungen erlauben		
Einrichten neuer Geräte in der Nähe erlauben		
Hinzufügen oder Entfernen einer Mobilfunkverbindung erlauben		
Ändern von Einstellungen für Mobilfunkverbindungen für Apps erlauben		
Ändern von Mobilfunkverbindungen erlauben		
Continuous Path Tastatur erlauben		
Automatisches Einstellen von Datum und Uhrzeit erzwingen		
Anzeigen von App-Clips erlauben		

Payload Domänen

Es besteht die Möglichkeit, Webdomänen (URLs) als verwaltet zu behandeln. Sensible Dateien, die auf einer Website verfügbar sind, können standardmäßig in die nicht verwalteten App-Bereiche heruntergeladen