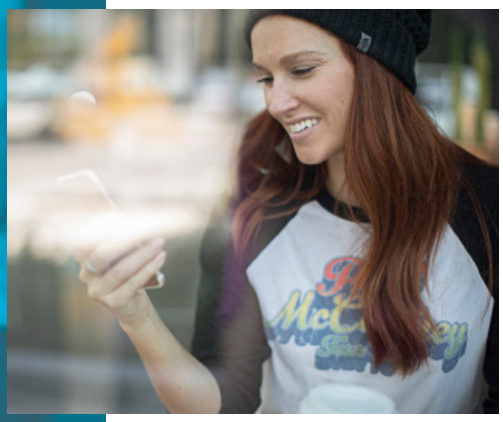
jamf

WHITEPAPER

Leitfaden zur Microsoft Enterprise Compliance



Mit iOS Geräte-Compliance wird die Partnerschaft zwischen Jamf und Microsoft ausgeweitet, sodass jetzt das gesamte Portfolio der Apple Enterprise Produkte unterstützt wird.

Arbeiten im Homeoffice, Fernunterricht und Telemedizin - die Sicherheit von Mobilgeräten ist jetzt wichtiger denn je. Ganz gleich, ob Ihre Organisation stationäre Patienten betreut oder Personal weltweit unterstützt: iOS und iPadOS Geräte sind oft der Schlüssel für Ihre Produktivitätsstrategie. Immer weniger Unternehmen nutzen ausschließlich Windows und immer mehr bieten ihren Mitarbeitern Wahlprogramme für ihre Arbeitsgeräte an. Daher ist es an der Zeit, Sicherheits-Workflows für Apple zu etablieren, die über den Sicherheits-Standard für Windows-Geräte hinausgeht.

iOS und iPadOS Geräte-Compliance (zusammenfassend als iOS Geräte-Compliance bezeichnet) ist eine wichtige Erweiterung der Partnerschaft zwischen Jamf und Microsoft.

Weitere Informationen:

Diese Microsoft Integration folgt auf den proxylosen bedingten Zugriff für Mac mithilfe von Jamf und Microsoft Enterprise Mobility + Security.

Vollständige Mac Workflow-Details von Microsoft und Jamf

Die Entwicklung der Partnerschaft zwischen Jamf und Microsoft

2017

Jamf und Microsoft kündigten eine völlig neuartige Partnerschaft an, um bedingten Zugriff für den Mac zu ermöglichen.

Jamf in Verbindung mit Microsoft Enterprise Mobility wie auch die Enterprise Mobiility Security (EMS) bietet eine automatisierte Compliance-Management-Lösung für Macs, die auf Anwendungen mit Azure AD-Authentifizierung zugreifen. Bei dieser Zusammenarbeit wird der bedingte Zugriff genutzt, um sicherzustellen, dass nur vertrauenswürdige Benutzer auf Unternehmensdaten zugreifen können.

2018

Jamf erweitert die Integration, um Endbenutzern eine nahtlosere Login-Erfahrung zu bieten.

Die Integration von Jamf und Microsoft Technologie bietet Endbenutzern eine nahtlosere Login-Erfahrung. Mit Jamf Pro, Jamf Connect und Microsoft Enterprise Mobility + Security (EMS) können Benutzer sich mit Microsoft Azure Active Directory Anmeldeinformationen bei einem neuen Mac anmelden, wodurch kein lokaler Benutzername und kein Passwort auf dem Mac des Endbenutzers mehr erstellt und verwaltet werden muss.

2020

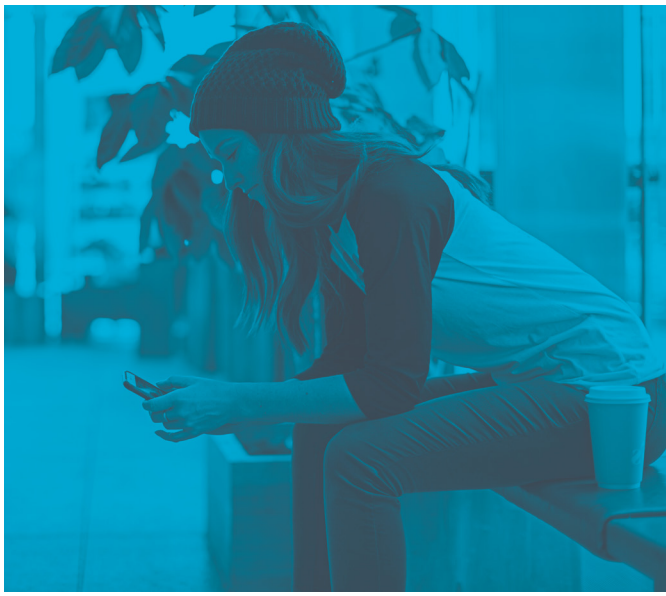
Jamf erweitert die Partnerschaft mit Microsoft mit Einführung des ersten bedingten Zugriffs für Apple Mobilgeräte auf dem Markt.

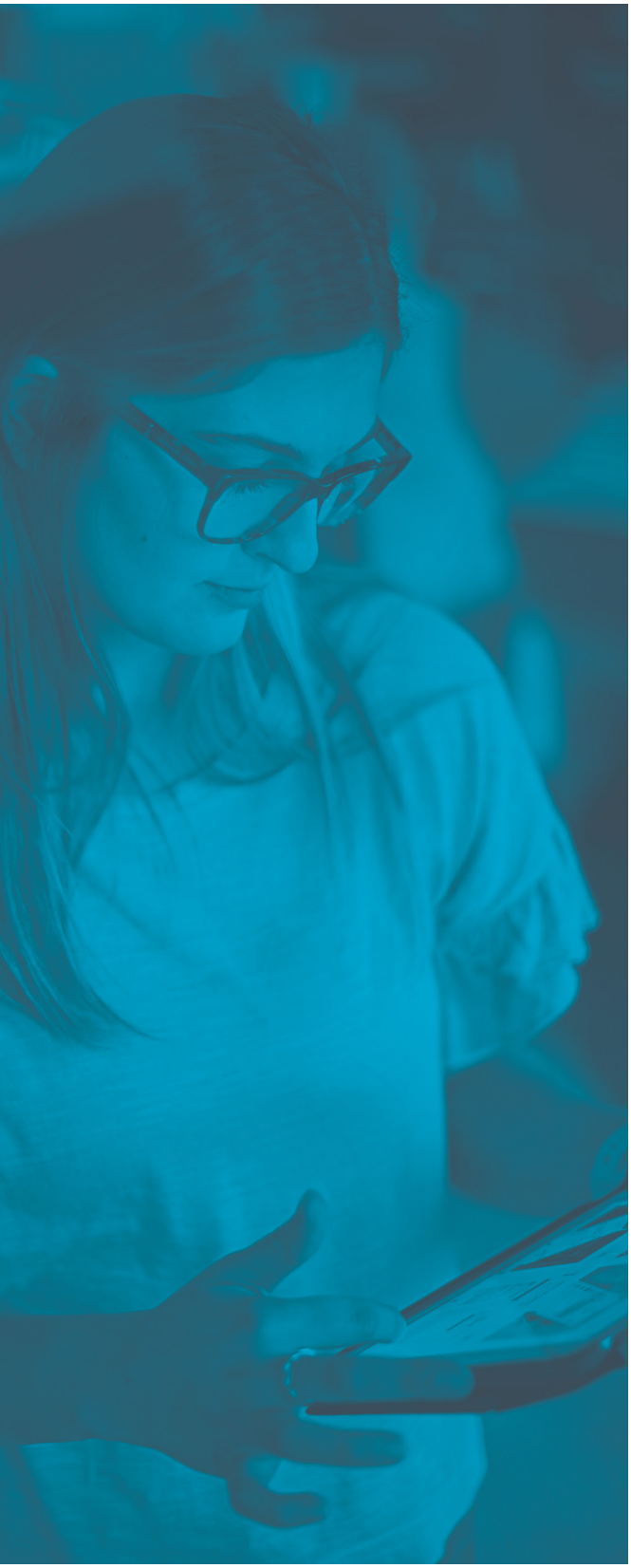
Unternehmen genießen bereits die Möglichkeit, bedingten Zugriff auf macOS Geräte zu nutzen, indem Bestandsdaten aus Jamf mit Microsoft Endpoint Manager geteilt werden. Die erweiterte Zusammenarbeit zwischen Jamf und Microsoft wird um iOS Unterstützung ergänzt. IT-Teams können jetzt verhindern, dass ein autorisierter Benutzer ein macOS oder iOS Gerät verwendet, das nicht mit den Sicherheitsrichtlinien konform ist, und können Jamf Self Service nutzen, um alle Apple Geräte zu schützen und zu unterstützen.

Wer iOS Geräte-Compliance benötigt

iOS Geräte-Compliance ist für alle gedacht. Jedem Unternehmen mit Apple und Microsoft bietet iOS Geräte-Compliance viele Vorteile. Insbesondere Unternehmen mit hybriden Umgebungen, etwa solche mit unterschiedlichen Teams für die IT und für die Informationssicherheit, profitieren von der erweiterten Integration und Kommunikation.

Unternehmen genießen bereits die Möglichkeit, bedingten Zugriff auf macOS Geräte zu nutzen, indem Bestandsdaten aus Jamf mit Microsoft Endpoint Manager geteilt werden. IT-Teams können jetzt verhindern, dass ein autorisierter Benutzer jedes beliebige iOS Gerät verwendet, das nicht den Sicherheitsrichtlinien ihres Unternehmens entspricht, und können Jamf Self Service für die Problembehebung nutzen.





So funktioniert's

Compliance-Kriterien festlegen:

Mit iOS Geräte-Compliance können Administratoren Compliance-Kriterien festlegen, um sicherzustellen, dass iOS Geräte Sicherheitsstandards erfüllen, bevor sie auf Unternehmensressourcen zugreifen können.

Umfang der Compliance-Kriterien bestimmen:

Mithilfe patentierter Smart Groups zur Umfangsbestimmung für die Compliance-Kriterien bestätigt Jamf Pro die Geräte-Compliance und sendet ein „Konform/Nicht konform“-Flag an Microsoft Azure AD.

Compliance-Meldung:

Die von Jamf erfassten Geräteinformationen werden dann an Azure AD gesendet. Weil Azure AD die von Jamf Pro gesendeten Informationen im Gerätedatensatz speichert und das Flag vor jedem einzelnen Zugriff auf Unternehmensressourcen wie OneDrive, Outlook usw. liest, bevor der Zugriff gewährt wird, werden Firmen-Assets, Daten und Ressourcen besser geschützt.

Problembehebung:

Wird ein Gerät als „nicht konform“ gekennzeichnet, wird der Zugriff verweigert und es müssen Maßnahmen getroffen werden, bevor der Endbenutzer den Vorgang fortsetzen kann. Der Endbenutzer, dessen Zugriff verweigert wurde, wird an Jamf Self Service weitergeleitet, um mit dem Prozess zu beginnen, damit er wieder richtlinienkonform wird.

Was anfangs benötigt wird

- Jamf Pro, mit Microsoft Endpoint Manager integriert
- Smart Group mit Geräten, die auf Compliance überwacht werden sollen
- Jamf Pro Benutzerkonto mit Berechtigungen für bedingten Zugriff
- Richtlinie für bedingten Zugriff, die vorgibt, dass Geräte als konform gekennzeichnet werden müssen, um auf die Ressourcen des Unternehmens zugreifen zu können
- Microsoft Enterprise Mobility + Security (speziell Microsoft AAD Premium und Microsoft Intune)

Um die Geräte-Compliance überwachen zu können, benötigen die Geräte:

- iOS 11 oder neuer bzw. iPadOS 13 oder neuer mit Safari als Standard-Browser
- Microsoft Authenticator App (im App Store erhältlich)
- Jamf Self Service für iOS 10.10.3 oder neuer

Das war's!

Unternehmen weltweit wird Zero-Trust-Geräte-Compliance immer wichtiger. Weil die Technologieerfahrung aufgrund der Telearbeit im Prinzip die gesamte Mitarbeitererfahrung ausmacht, kann die Bedeutung von Compliance und Sicherheit gar nicht überbetont werden.

iOS Geräte-Compliance mit Apple und Microsoft – den Standards in Unternehmen – sorgt für die Verbesserung der Sicherheit und Verwaltung Ihrer iOS Geräte, stellt die Geräte-Compliance sicher und unterstützt alle Apple Geräte in Ihrem Unternehmen.

Legen Sie noch heute los

Aktuelle Kunden, die Jamf Cloud nutzen, sehen diese Integration in Jamf Pro als „iOS Geräte-Compliance“ im Menü „Globales Management“. Weitere Informationen über dieses neue Feature finden Sie in unserem **technischen Leitfaden.**

Falls Sie noch kein Jamf Kunde sind, können Sie eine kostenlose Testversion anfordern, oder kontaktieren Sie Ihren bevorzugten Apple Partner.

Testversion anfordern