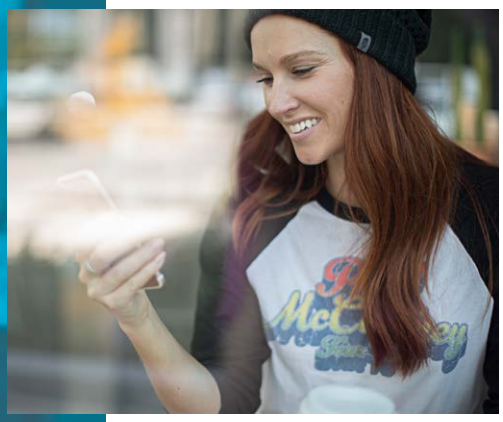
jamf

WHITE PAPER

Steps to Complete Microsoft Enterprise Compliance



Device Compliance for iOS expands the Jamf and Microsoft partnership to support the entire Apple enterprise fleet.

Remote work, learning and healthcare has made mobile device security more important than ever. Whether your organization is delivering care for patients down the hall or supporting staff around the world, iOS and iPadOS devices are often a key part of your productivity strategy. With the enterprise no longer Windows-centric and more employee choice programs in place, it's time to elevate your Apple security workflows to the same standard as you non-Apple environments.

Device Compliance for iOS and iPadOS (commonly referred to as Device Compliance for iOS) is a significant expansion to Jamf's partnership with Microsoft.

Learn more:

This Microsoft integration follows proxy-free conditional access for Mac made possible by Jamf and Microsoft Enterprise Mobility + Security.

Full Mac workflows details from Microsoft and Jamf

The evolving Jamf and Microsoft partnership

2017

Jamf and Microsoft announced a first-of-its-kind partnership to bring Conditional Access to the Mac.

Jamf and Microsoft Enterprise Mobility + Security (EMS) partnership, which provides an automated compliance management solution for Mac devices accessing applications set up with Azure AD authentication. This collaboration leverages conditional access to ensure that only trusted users are accessing company data.

2018

Jamf expanded its integration to create a more seamless login experience for end users.

Jamf and Microsoft technology integration that offer a more seamless login experience for end users. With Jamf Pro, Jamf Connect and Microsoft Enterprise Mobility + Security (EMS), users can log in to a new Mac with Microsoft Azure Active Directory credentials, eliminating the need to create and manage a local username and password on an end user's Mac.

2020

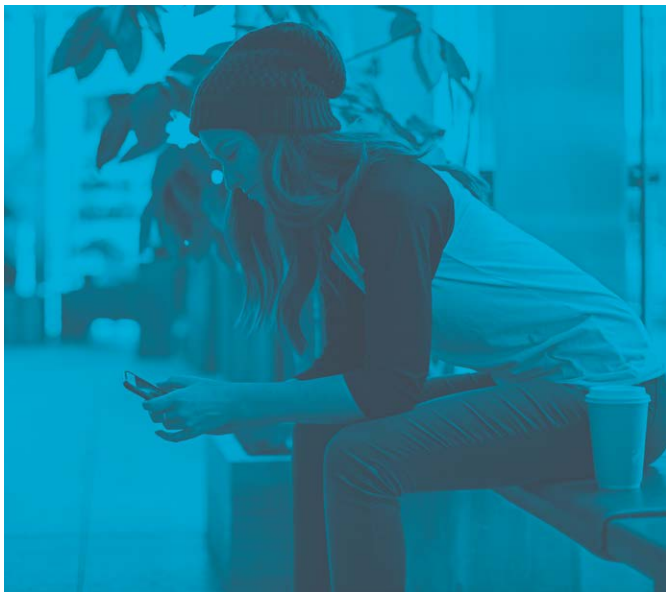
Jamf further expanded its partnership with Microsoft first-to-market conditional access for Apple mobile devices.

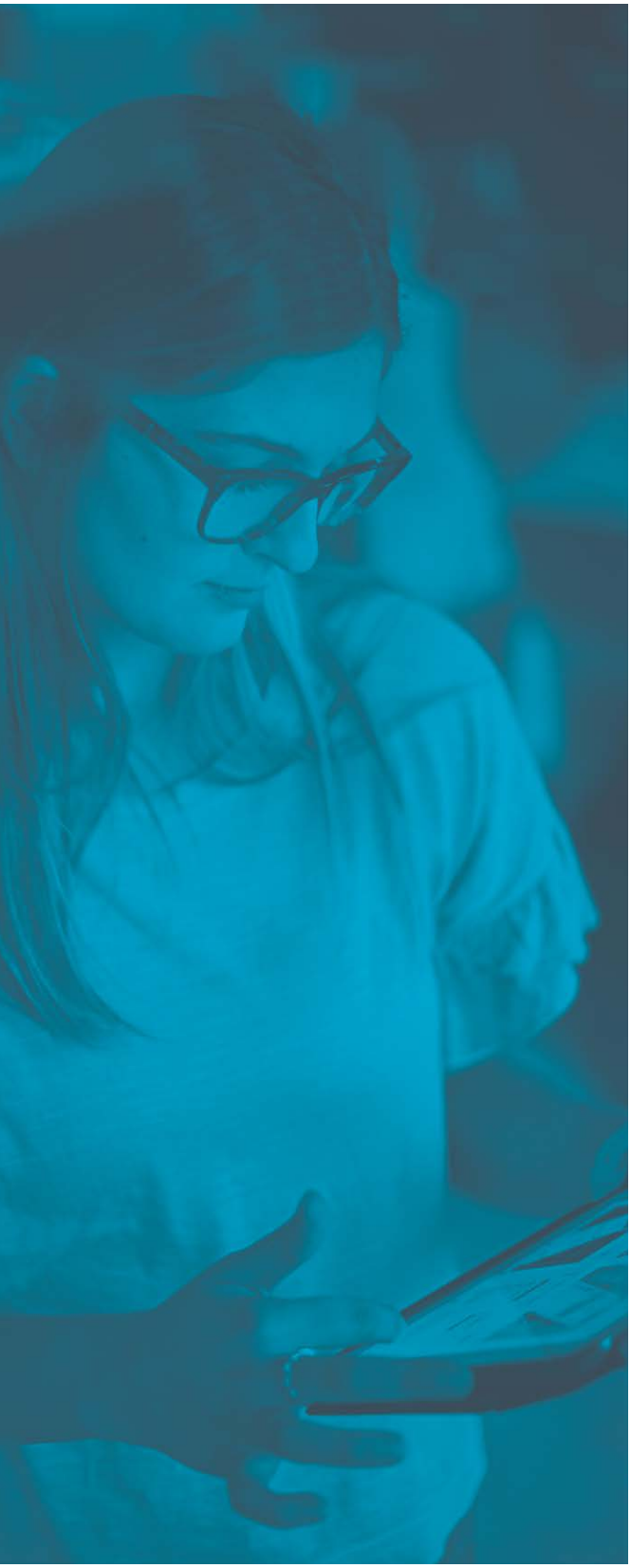
Organizations already enjoy the ability to leverage Conditional Access on macOS devices, by sharing inventory data from Jamf with Microsoft Endpoint Manager. The expanded collaboration between Jamf and Microsoft adds iOS support. Now IT teams can prevent an authorized user from using any macOS or iOS device that does not comply with security policies, and leverage Jamf Self Service for remediation to secure and support their entire fleet of Apple devices.

Who needs Device Compliance for iOS

Device Compliance for iOS is for everyone. Organizations with hybrid environments, organizations with different leads for IT and Information Security teams, any organization with Apple devices and Microsoft will benefit from Device Compliance for iOS.

Organizations already enjoy the ability to leverage Conditional Access on macOS devices by sharing inventory data from Jamf with Microsoft Endpoint Manager. Now IT teams can prevent an authorized user from using any iOS device that does not comply their organization's security policies and leverage Jamf Self Service for remediation.





How it works

Establish compliance criteria:

With Device Compliance for iOS, admins can establish compliance criteria to ensure that iOS devices meet security standards before accessing organizational resources.

Scope compliance criteria:

Leveraging patented Smart Groups to scope compliance criteria, Jamf Pro verifies device compliance and then passes a “compliant / not compliant” flag back to Microsoft Azure AD.

Report compliance:

The device information collected by Jamf is then sent to Azure AD. Because Azure AD holds the information scoped by Jamf Pro on the device record and reads the flag before granting access for each and every sign in to company resources, like OneDrive, Outlook, etc., company assets, data and resources are better protected and secure.

Remediate:

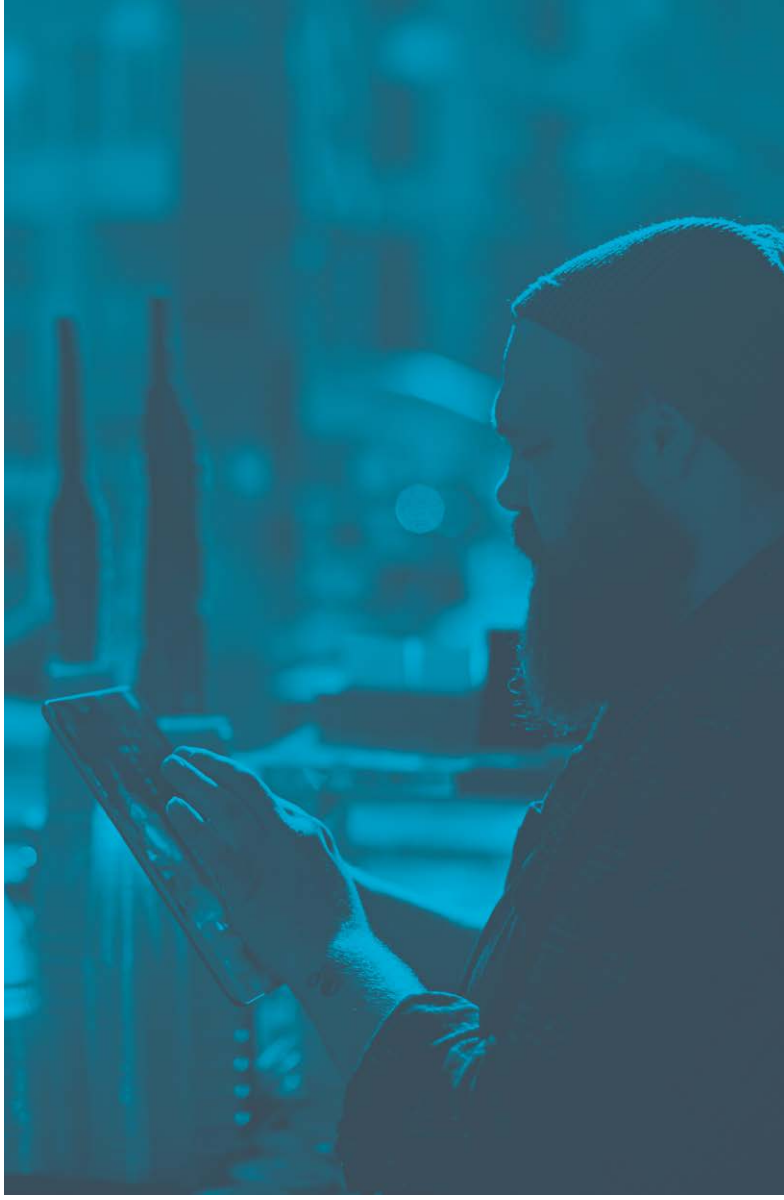
If a device is flagged “not compliant,” access is denied and remediation is required for the end user to continue. The denied end user is directed to Jamf Self Service to begin the remediation process to be brought back into compliance.

What you need to get started

- Jamf Pro integrated with Microsoft Endpoint Manager
- Smart device group that contains the devices you want to monitor for compliance
- Jamf Pro user account with Conditional Access privileges
- A Conditional Access policy to require devices be marked as compliant in order to access your organization’s resources
- Microsoft Enterprise Mobility + Security (specifically Microsoft AAD Premium and Microsoft Intune)

In order to monitor device compliance, the devices must have:

- iOS 11 or later, or iPadOS 13 or later with Safari set as the default browser
- Microsoft Authenticator App (available in the App Store)
- Jamf Self Service for iOS 10.10.3 or later



Ready, set, compliance

Organizations all around the world are seeing a need for zero-trust device compliance and, with the technology experience being the entire employee experience for a remote workforce, the importance of compliance and security cannot be overstated.

Device Compliance for iOS with Apple and Microsoft — the standards in enterprise business — advances your ability to secure and manage your iOS devices, ensure device compliance and support your enterprise Apple fleet.

Get started today

For current customers using Jamf Cloud, this new integration will appear in Jamf Pro as Device Compliance for iOS under the Global Management menu. For additional information and assistance leveraging this new feature, see our **technical guide.**

If you haven't joined Jamf yet, request a free trial or contact your preferred Apple reseller to get started.

Request Trial