jamf

Definitiver Leitfaden für **Jamf und Cisco** im Unternehmen

Cisco verbindet und sichert Endbenutzer*innen mit den Netzwerken und Ressourcen, die sie für ihren Erfolg benötigen, unabhängig davon, wo sie sich befinden. Netzwerkinfrastruktur, Sicherheitstools und Apps für Endbenutzer*innen arbeiten zusammen, um eine sichere Umgebung zu schaffen und Ihre Organisation zu unterstützen. In einer Welt, die zunehmend von mobilen Benutzer*innen und Netzwerken abhängt, sind Sicherheitstools für Netzwerke und Lösungen, die Produktivität, Zusammenarbeit und Mitarbeiterzufriedenheit unterstützen, unerlässlich.

Als **dominierender Akteur in der Welt** der Unternehmensnetzwerke ist es durchaus möglich, dass Cisco bereits die bevorzugte Lösung für Ihr Unternehmen ist. Oder vielleicht haben Sie gerade erst mit der Suche nach dem besten Technologie-Stack für Ihre auf Apple ausgerichtete Organisation begonnen. Unabhängig davon, wo Ihre Organisation in Bezug auf ihre Netzwerksysteme angesiedelt ist, erläutern wir Ihnen hier, wie Jamf und Cisco integriert sind und erstklassige Lösungen anbieten, die das Netzwerk, die Sicherheit, die Geräteverwaltung, die Produktivität und die IT-Transparenz Ihrer Organisation verbessern.

Gemeinsam machen Jamf und Cisco das Beste aus Ihren IT-Investitionen. Durch Produktintegrationen und unseren speziellen Fokus auf Apple profitieren Ihre Benutzer*innen von einem nahtlosen und sicheren Zugriff auf die wichtigen Ressourcen.

In diesem Leitfaden geben wir einen Überblick über die Jamf Cisco Integrationen, die die Apple Fleet Ihrer Organisation unterstützen.

Inhaltsverzeichnis:

Cisco ISE

Cisco SecureX

Fastlane+

DUO

Cisco DNA

WebEx

Integrationen

Cisco ISE

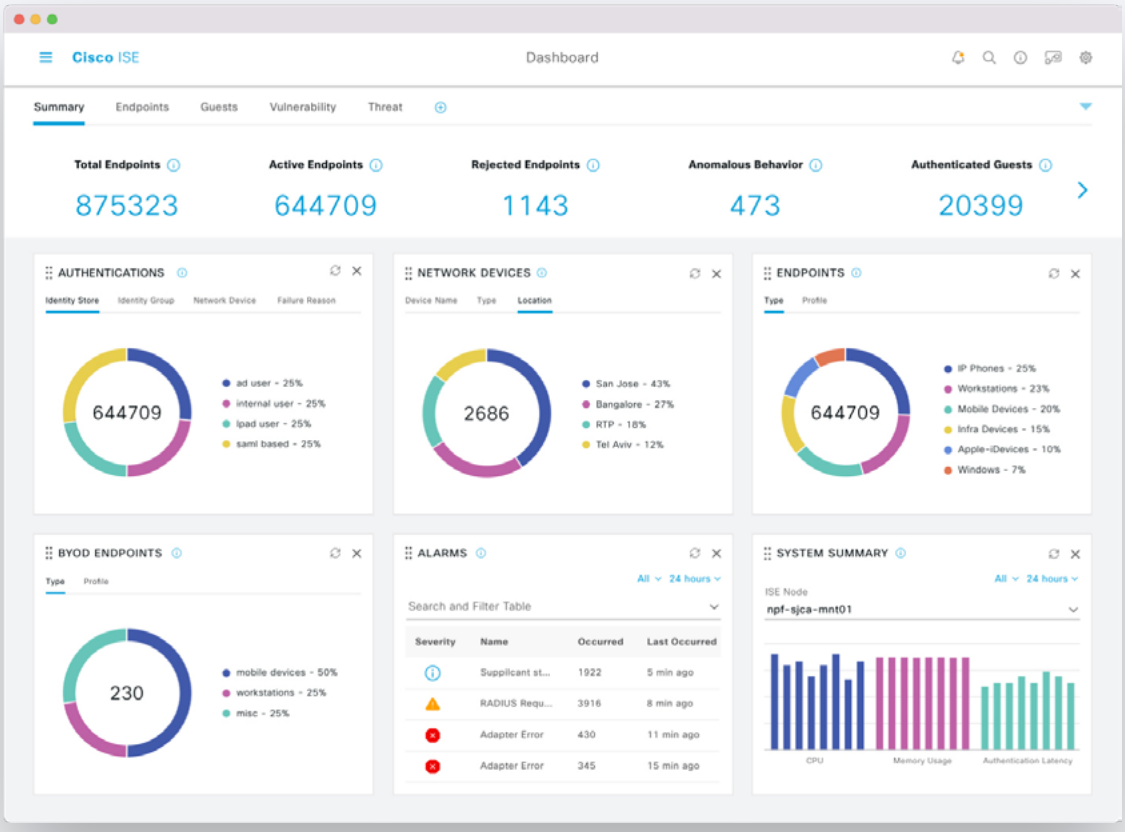
beginnt mit dem Netzwerk

Die Cisco Identity Services Engine (ISE) bietet einen hochsicheren Netzwerk-Zugang für Benutzer*innen und Geräte mit einer Zero-Touch-Strategie. Verschaffen Sie sich Transparenz über die Vorgänge in Ihrem Netzwerk, z. B. darüber, wer verbunden ist, welche Apps installiert sind und ausgeführt werden, und vieles mehr, und automatisieren Sie die Durchsetzung von Richtlinien. Durch die Integration mit den Verwaltungsfunktionen von Jamf können Sie die Leistungsfähigkeit von Cisco ISE erweitern, um Bedrohungen schneller und effizienter zu identifizieren, einzudämmen und zu beheben.

Wie? Es ist ganz einfach.

Die Netzwerk Integration mit Cisco ISE ermöglicht es dem Service, mit Jamf Pro zu kommunizieren und zu überprüfen, ob die Computer und Mobilgeräte in Ihrem Netzwerk den Standards Ihrer Organisation entsprechen. Sobald die Daten von Jamf Pro erfasst sind, kann der Dienst den Grad des Netzwerkzugriffs bestimmen, der einem Computer oder Mobilgerät gewährt werden soll, Endnutzer*innen Nachrichten zur Verfügung stellen und Endnutzer*innen anweisen, ihre Computer und Mobilgeräte bei Jamf Pro zu registrieren, um sicherzustellen, dass nur konforme Geräte und Nutzer*innen auf Ihr Netzwerk zugreifen.

Diese Integration ermöglicht es dem Netzwerkzugriffsverwaltungsdienst auch, Remote-Befehle an Computer und Mobilgeräte über Jamf Pro zu senden, einschließlich Passcode-Sperr- und Löschbefehle, um die Unterstützung und Sicherheit Ihrer Geräte und Ihres Netzwerks zu gewährleisten.



Cisco SecureX

Device Einblicke für mehr Transparenz über alle Ihre Tools hinweg

Device Insights von Cisco SecureX vereint mehrere Geräteverwaltungen, Endgeräte-Erkennung und -Reaktion, Antivirus (AV) und andere Endgerätesicherheitsprodukte, um die Details, die diese Tools und Lösungen liefern, in einer einheitlichen Ansicht innerhalb von SecureX zu konsolidieren.

Mithilfe von Geräteeinblicken können Sie die Anzahl der Gerätebestände verfolgen und die wachsende und sich verändernde Natur Ihres Netzwerks besser verstehen. Darüber hinaus können Sie mit der Endgerätesuche und dem Reporting den Sicherheitsstatus von Geräten im Besitz von Mitarbeitern*innen, Auftragnehmer*innen und IoT/OT-Geräten bewerten, ohne eine Unterbrechung des Unternehmens zu riskieren. Stoppen Sie Bedrohungen, bevor Probleme auftreten!

Gängige IT-Probleme im Zusammenhang mit der Verwaltung von Beständen und Anlagen lassen sich ebenso einfach lösen wie Netzwerkprobleme, da Sie einen Überblick über alle mit dem Netzwerk verbundenen Geräte haben. Durch die Nutzung der Verbindung zwischen den Dashboards von Cisco und Jamf können Administrator*innen schnell von SecureX zu Jamf Pro zurückkehren, um Risiken zu minimieren und Probleme, die bei Apple Endgeräten erkannt wurden, zu lösen. Dies erlaubt es der IT-Abteilung, auf Workflows zur Behebung von Problemen umzuschwenken und diese als Teil eines einzigen, zusammenhängenden Verfahrens anzugehen.

*Benutzer*innen können zwischen Dunkel- und Hellmodus wählen*

Fastlane+

Ein intelligentes Netzwerk für Apple Geräte

Fastlane+, entwickelt von Cisco und Apple, ist eine Lösung, die die Erfahrung aller WLAN 6 fähigen Apple iOS/iPadOS Geräte, die mit einem Cisco Wireless WLAN 6 Netzwerk verbunden sind, deutlich verbessert. Durch die Nutzung der OFDMA-Technologie von WLAN 6 bietet Fastlane+ den Benutzer*innen eine unglaubliche Sprach- und Videostreaming-Qualität, selbst in den überlastetsten Umgebungen für Clients mit iOS 14 oder höher. Fastlane+ erweitert die bestehende Fastlane-Lösung, optimiert das Roaming von iOS Clients mit adaptivem 802.11r und erlaubt Benutzer*innen, bestimmte Sprach- und Video-Apps zu priorisieren.

Mit Fastlane+ identifizieren Organisationen, welchen Apps sie in ihrem Netzwerk Priorität einräumen wollen. Nachdem ein Netzwerk für Cisco Fastlane+ konfiguriert wurde, müssen Unternehmen eine Enterprise oder eine Mobile Device Management (MDM)-Lösung wie Jamf verwenden, um die Konfiguration auf Geräteebene durchzuführen.

Mit Jamf Pro können Unternehmen die identifizierten prioritären Apps auf jedem verwalteten Gerät oder in Gruppen von Geräten durchsetzen und so sicherstellen, dass bei einer Überlastung des Netzwerks nicht-kritische Apps die Leistung der wichtigen Apps nicht beeinträchtigen.

DUO

Erhöhte Sicherheit für Endgeräte

Mit der Funktion „Vertrauenswürdige Endgeräte” von Duo können Sie vertrauenswürdige Endgeräte definieren und verwalten und den sicheren Zugriff auf die Apps Ihrer Organisation mit Richtlinien gewähren, die Systeme anhand von Gerätezertifikaten, Anwendungsüberprüfung oder Verwaltungsstatus verifizieren. Duo unterstützt Organisationen bei der Unterscheidung zwischen nicht verwalteten und verwalteten Endgeräten, die auf Ihre browserbasierten Apps zugreifen.

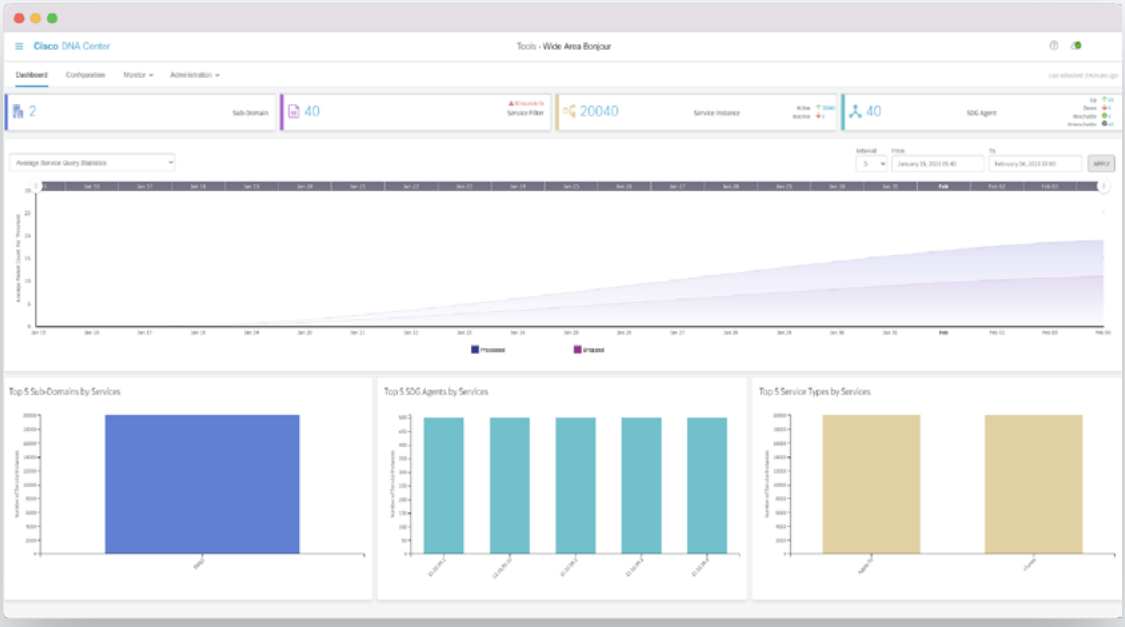
Mit der Integration von Jamf Pro identifiziert Trusted Endgeräte, welche Clients auf die Apps zugreifen, die verwaltet werden, und blockiert den Zugriff auf verschiedene Apps von nicht verwalteten Systemen. Benutzer*innen authentifizieren sich bei Apps, die mit der browserbasierten Eingabeaufforderung von Duo geschützt sind. Anschließend gleicht Duo die von der App Device Health gemeldeten Geräte-Identifikatoren mit den von Jamf über eine nächtliche Synchronisierung mit schreibgeschützter API verwalteten Geräte-Informationen ab.

Cisco DNA

Adaptieren Sie erstaunliche Funktionen von Apple für Ihr Netzwerk

Die Cisco Digital Network Architecture (Cisco DNA) hat es geschafft, Netzwerke im Unternehmen zu vereinfachen und für Kund*innen intuitiver zu gestalten. Die Cisco DNA Service für Bonjour Lösung ermöglicht das Routing von mDNS-Diensten für Apple oder Industriestandard-basierte Geräte. Die Wide-Area-Bonjour-Funktionen unterstützen End-to-End-Unicast-basiertes Service-Routing mit unternehmensgerechter Skalierung und Sicherheit bei gleichzeitiger Aufrechterhaltung einer konsistenten Benutzererfahrung in privaten oder erstklassigen Unternehmensnetzwerken.

Schulen mit Apple Geräten in ihrem Netzwerk benötigen eine Möglichkeit, die Fähigkeiten der Apple Geräte in ihren Netzwerken auf skalierbare Weise zu optimieren, um eine anpassbare, personalisierte Erfahrung zu bieten. Die Cisco DNA Lösung unterstützt Zusammenarbeit, Content Sharing und IoT Geräte. Lehrkräfte können nun Inhalte und Apps mit ihren Schüler*innen teilen, und die Schüler können eine Streaming-Technologie wie AirPlay nutzen, um miteinander zusammenzuarbeiten, ohne dass es zu Problemen kommt, die normalerweise in größeren Netzwerken auftreten.

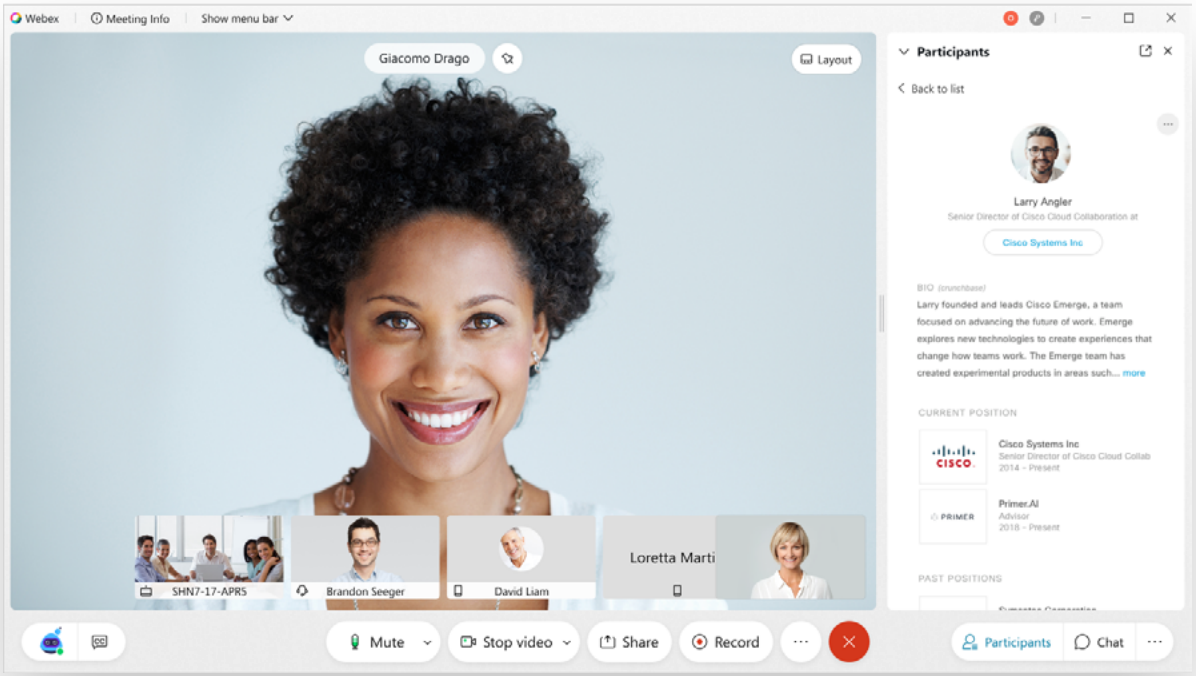


WebEx

Einrichtung und Konfiguration

WebEx unterstützt die Zusammenarbeit. Von den allgemeinen Grundlagen der Kommunikation, wie Video und Sprache, bis hin zu fortgeschrittenen Funktionen, mit denen Teams aus der Ferne nahtlos arbeiten können, wie Whiteboarding und Augmented Reality (AR), unterstützt WebEx jede Art von Projekt.

Mit Jamf ermächtigt WebEX die Benutzer*innen, diese Werkzeuge zu nutzen. Durch diese Integration wird die Lösung für die Anforderungen Ihres Unternehmens verfügbar und konfiguriert und stellt darüber hinaus sicher, dass sie auf den verwalteten Macs und mobilen Geräten der Benutzer*innen auf dem neuesten Stand ist. Jamf's Fähigkeiten im **App-Lifecycle Management** machen es einfach, sicherzustellen, dass die richtigen Apps und Versionen immer auf dem Gerät eines Benutzers/einer Benutzeri sind. Darüber hinaus kann Jamf die WebEx-Erfahrung auf dem iPad so anpassen, dass sie für einen bestimmten Benutzer-Account vorkonfiguriert ist. Dies ist äußerst hilfreich bei virtuellen Telehealth Workflows für Patient*innen und Mitarbeiter*innen und in anderen Situationen, in denen ein kioskähnliches Gerät benötigt wird. Die Fähigkeit von Jamf, Apps vorkonfigurieren zu können, basiert auf unserer Unterstützung von AppConfig, einer leistungsstarken Funktion von MDMs zum Laden von Einstellungen, Anmeldedaten und mehr zusammen mit der App. Diese Kombination aus App-Bereitstellung, Aktualisierungen und Verwaltung von Einstellungen führt zu einer vereinfachten Benutzererfahrung, bei der die Benutzer*innen sofort von der WebEx-Plattform profitieren können.



Wir wissen, dass dies eine Menge sein könnte.

Und so viel ist möglich, wenn Sie Jamf — den Standard im Apple Enterprise Management — mit Cisco kombinieren. Probieren Sie also Jamf kostenlos aus und überzeugen Sie sich selbst. Wir helfen Ihnen auf dem Weg dorthin.

Fordern Sie eine Testversion an oder wenden Sie sich an Ihren bevorzugten Apple Reseller, um loszulegen.