



# Guide de Jamf et Cisco dans l'entreprise



Cisco connecte en toute sécurité les utilisateurs finaux aux réseaux et aux ressources dont ils ont besoin pour réussir, où qu'ils soient. L'infrastructure du réseau, les outils de sécurité et les applications métier forment ensemble un environnement sécurisé qui soutient vos activités. Et dans un monde qui compte de plus en plus sur les utilisateurs et les réseaux mobiles, il faut des outils qui sécurisent les réseaux et des solutions axées sur la productivité, la collaboration et la satisfaction des employés.

En tant qu'**acteur dominant dans le monde des réseaux d'entreprise**, il se peut que Cisco soit déjà la solution de référence de votre organisation. Mais il se peut aussi que vous soyez encore en quête de la meilleure technologie pour votre organisation orientée Apple. Dans tous les cas, l'intégration de Jamf et Cisco peut être un atout pour votre entreprise. Ensemble, nous délivrons des solutions de pointe pour améliorer les performances du réseau, la sécurité, la gestion des appareils, la productivité et la visibilité informatique.

Combiner Jamf et Cisco, c'est exploiter pleinement l'investissement informatique de votre entreprise. Grâce aux intégrations de produits et à notre alignement Apple, vos utilisateurs bénéficieront d'un accès simple et sécurisé aux ressources essentielles.

Dans ce guide, vous découvrirez les intégrations Jamf-Cisco qui prennent en charge la flotte Apple de votre organisation.

## Table des matières

[Cisco ISE](#)

[Cisco SecureX](#)

[Fastlane+](#)

[DUO](#)

[Cisco DNA](#)

[WebEx](#)

# Intégrations

## Cisco ISE

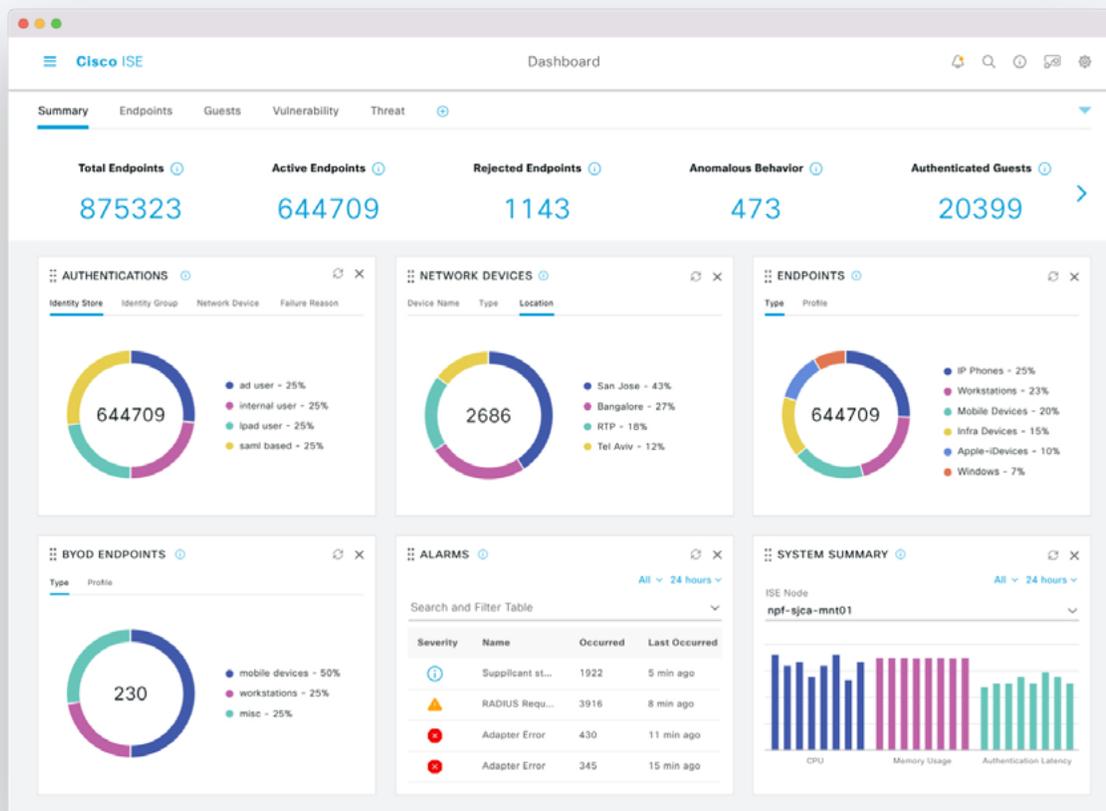
### Tout commence par le réseau

Cisco Identity Services Engine (ISE) offre un accès réseau hautement sécurisé aux utilisateurs et aux appareils selon une stratégie zero-touch. Vous bénéficiez d'une visibilité totale sur ce qui se passe dans votre réseau : qui est connecté, quelles applications sont installées et en cours d'exécution, etc. Et vous pouvez appliquer des règles de façon automatisée. Et quand Cisco ISE est intégré aux capacités de gestion des appareils de Jamf, vous pouvez identifier, contenir et corriger les menaces plus rapidement et plus efficacement.

Comment ? C'est simple.

L'intégration réseau avec Cisco ISE permet au service de communiquer avec Jamf Pro, et donc de vérifier que les ordinateurs et appareils mobiles du réseau sont conformes à vos standards. Muni des données collectées par Jamf Pro, le service établit le niveau d'accès au réseau à accorder à un ordinateur ou à un appareil mobile. Il peut aussi transmettre des messages aux utilisateurs et les aider à inscrire leurs appareils dans Jamf Pro. Le résultat : votre réseau n'est accessible qu'aux appareils et aux utilisateurs conformes.

Cette intégration a un autre avantage : le service de gestion des accès au réseau peut envoyer des commandes à distance aux ordinateurs et aux appareils mobiles via Jamf Pro. Ces commandes – verrouillage par code et effacement, notamment – sont essentielles pour la prise en charge et la sécurité de vos utilisateurs et de votre réseau.



## Cisco SecureX

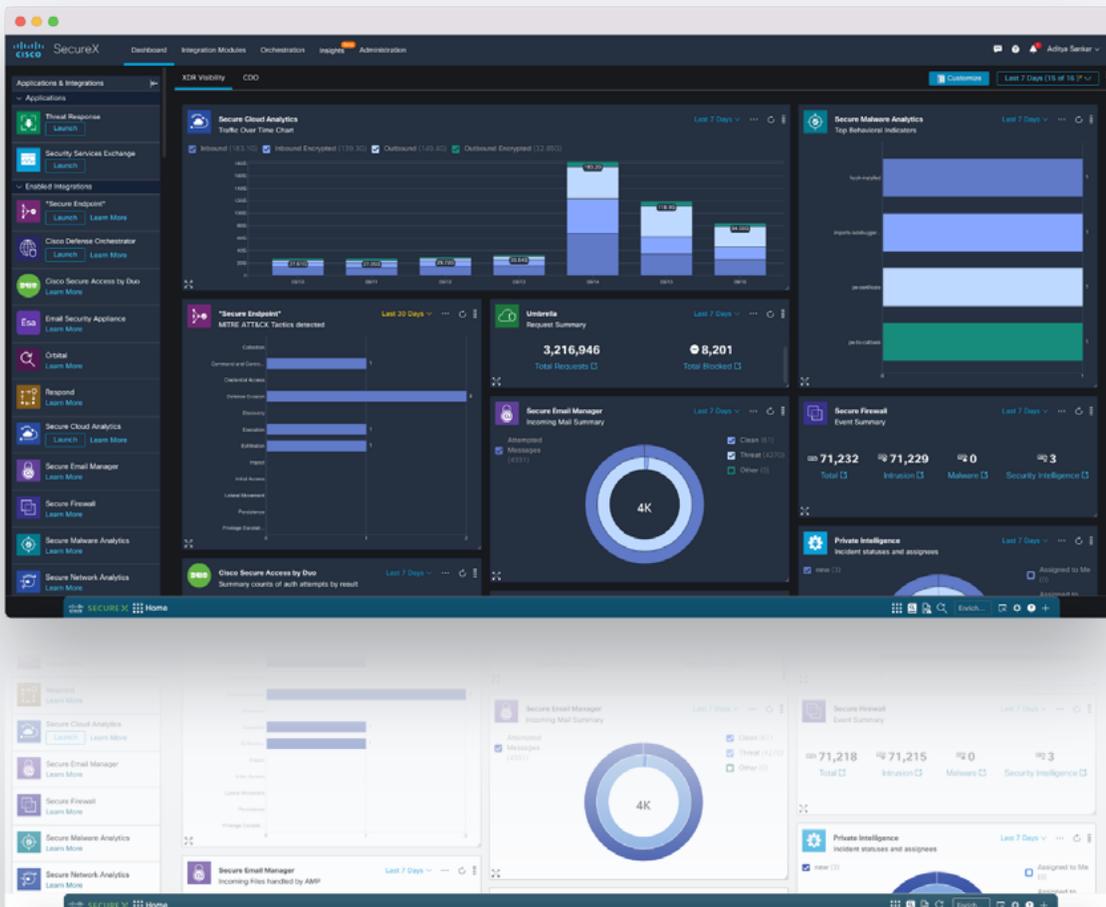
### Device Insights pour plus de visibilité sur votre parc

Module de Cisco SecureX, Device Insights unifie les outils de gestion des appareils, de détection et de réponse, d'antivirus (AV) et autres produits de sécurité des terminaux. Il rassemble toutes les informations fournies par ces solutions dans une vue unifiée au sein de SecureX.

Device Insights permet de tenir l'inventaire des appareils, pour mieux comprendre l'expansion et l'évolution de votre réseau. Grâce à ses fonctions de découverte et de rapports sur les terminaux, vous pouvez évaluer la posture de sécurité de tous les types d'appareils – ceux des employés et sous-traitants comme ceux de l'IoT et de l'OT. Et tout cela sans risquer de perturber les activités. Arrêtez les menaces avant que les problèmes ne surviennent

Les problèmes informatiques courants liés à la gestion de l'inventaire et des actifs sont tout aussi faciles à résoudre que les problèmes de réseau : tous les appareils connectés au réseau sont rassemblés au sein d'une vue unique.

Les tableaux de bord de Cisco et de Jamf sont liés : les administrateurs peuvent ainsi passer de SecureX à Jamf Pro pour atténuer les risques et hiérarchiser les problèmes détectés sur les terminaux Apple. L'équipe informatique bascule rapidement sur les workflows de correction et traite les problèmes en suivant processus cohérent.



Interface utilisateur disponible en mode sombre et en mode clair

## Fastlane+

### Un réseau intelligent pour les appareils Apple

Développé par Cisco et Apple, Fastlane+ améliore considérablement l'expérience des appareils Apple iOS/iPadOS compatibles Wi-Fi 6 qui sont connectés à un réseau Wi-Fi 6 de Cisco. Fastlane+ s'appuie sur la technologie OFDMA du Wi-Fi 6 : les utilisateurs sous iOS 14 et plus jouissent d'une incroyable qualité de streaming vocal et vidéo, même dans les environnements RF très fréquentés. Fastlane+ est une version améliorée de la solution Fastlane. Elle optimise l'itinérance des clients iOS grâce à la norme adaptative 802.11r et autorise les utilisateurs à donner la priorité à certaines applications vocales et vidéo.

Avec Fastlane+, les organisations peuvent privilégier des applications sur leur réseau. Une fois Cisco Fastlane+ est activé sur un réseau, une solution d'entreprise ou de gestion des appareils mobiles (MDM) telle que Jamf permettra de le configurer au niveau des appareils.

Avec Jamf Pro, les entreprises appliquent la hiérarchisation des applications aux appareils gérés, individuellement ou en groupe. Grâce à cela, quand le réseau est encombré, les applications non critiques n'ont pas d'impact sur les performances des outils importants.



# DUO

## Une sécurité renforcée pour les terminaux

La fonctionnalité Trusted Endpoints de Duo permet de définir et gérer des terminaux de confiance. Elle sécurise l'accès aux applications d'entreprise via des règles qui vérifient les appareils à l'aide de certificats, du contrôle des applications ou de l'état de gestion. Duo fait la distinction entre les terminaux gérés et non gérés qui accèdent à vos applications web.

Grâce à l'intégration de Jamf Pro, Trusted Endpoints reconnaît les clients gérés et bloque l'accès des systèmes non gérés à diverses applications. Les utilisateurs s'authentifient auprès des applications protégées par une boîte de dialogue Duo dans le navigateur. Grâce à une synchronisation nocturne avec Jamf effectuée via une API en lecture seule, Duo reçoit des informations sur les appareils, qu'il associe aux identifiants rapportés par l'application Device Health

The screenshot displays the Duo dashboard interface. At the top, there is a search bar and user information for 'Acme Corp | ID: 1234-5678-90 | Jewel Newport'. The main dashboard area is divided into several sections:

- Users:** 23 Bypass Users, 0 Locked Out, 491 Inactive. Total Users: 4.1k.
- Endpoints:** 661 Out of Date OS (6.7% increase in the last 7 days), 4.9k Up to Date, 5.8k Total Endpoints.
- Administrators:** 195 Administrators.
- 2FA Devices:** 4264 2FA Devices.
- Groups:** 121 Groups.
- Security Events:** 13.9k New Trust Monitor Security Events, including 2.7k Priority Events.
- Remaining Telephony Credits:** 2.4k.

A bar chart titled '9.8k Authentications' shows activity over the last 48 hours. The chart has two peaks: one around 11 AM on Saturday, August 14, and a larger one around 11 AM on Sunday, August 15.

The 'Authentication Log' section shows the last 10 attempts:

Timestamp (PDT)	Result	User	Application	Access Device	Second Factor
12:15:46 PM AUG 10, 2021	✔ Granted Valid passcode	belinda	LotusSpa	> Mac OS X 10.15.7 (19H1030) As reported by Device Health	> Yubikey Passcode Location Unknown

The 'What's New?' section features a notification for August 12th, 2021, regarding the 'Duo Universal Prompt' which is now available for public preview.

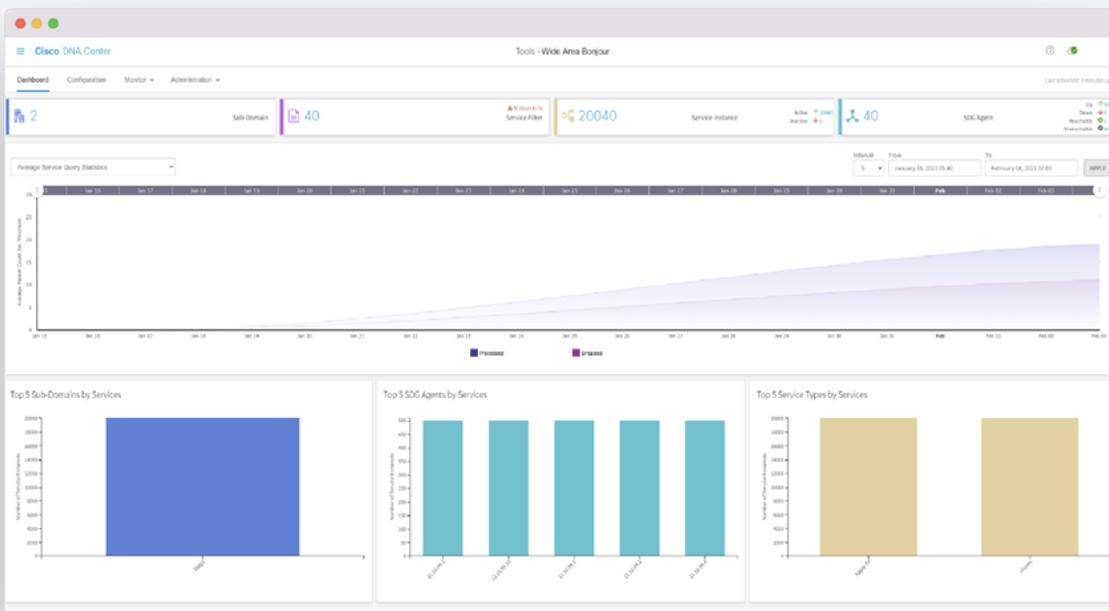


## Cisco DNA

### Adapter les fonctionnalités exceptionnelles d'Apple à votre réseau

L'architecture de réseau numérique de Cisco (Cisco DNA) simplifie les réseaux des grandes entreprises et les rend plus intuitifs pour les clients. La solution Cisco DNA Service for Bonjour assure l'acheminement du service mDNS pour les appareils Apple et ceux qui utilisent les standards de l'industrie. Les fonctionnalités Wide Area Bonjour prennent en charge l'acheminement de services Unicast de bout en bout à grande échelle. Elles garantissent une sécurité de niveau entreprise et préservent la cohérence de l'expérience utilisateur finale cohérente dans les contextes résidentiels comme dans les réseaux d'entreprise haut de gamme.

Les écoles équipées d'appareils Apple ont besoin d'un moyen d'harmoniser leurs capacités réseau avec souplesse afin d'offrir une expérience individualisée. La solution Cisco DNA prend en charge la collaboration, le partage de contenu et les appareils IoT. Grâce à elle, les enseignants partagent des contenus et des applications avec leurs élèves. Les technologies de diffusion en continu comme AirPlay facilitent la collaboration en classe, sans les problèmes traditionnellement associés aux réseaux plus vastes.

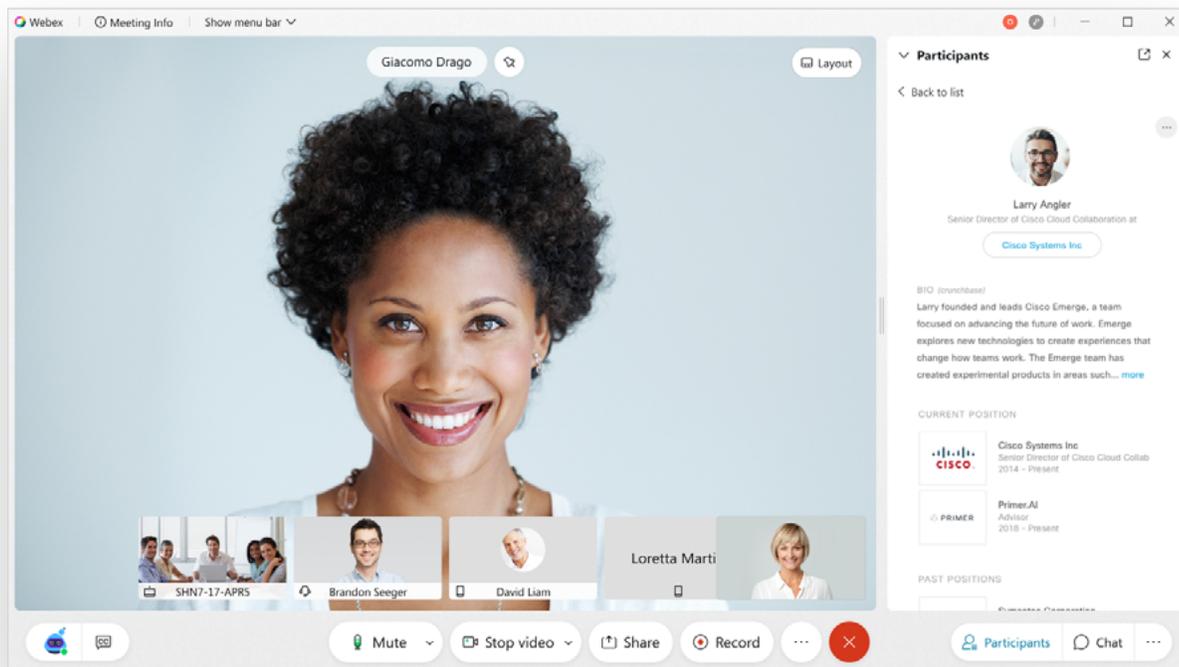


## WebEx

### Déploiement et configuration

WebEx encourage la collaboration. Des outils de communication de base, comme la vidéo et la voix, aux fonctionnalités avancées – tableau blanc, réalité augmentée – qui fluidifient le travail collaboratif à distance, WebEx prend en charge tout type de projet.

Avec Jamf, WebEX donne aux utilisateurs les moyens de profiter pleinement de ces outils. Cette intégration facilite la configuration et la mise à disposition de la solution, qui reste toujours à jour sur les Mac et les appareils mobiles gérés des utilisateurs. Grâce aux excellents outils Jamf de **Gestion du cycle de vie des applications**, vous aurez toujours la certitude que chaque appareil possède les bonnes applications, dans la version voulue. Pour aller encore plus loin, Jamf peut personnaliser l'expérience WebEx sur iPad en préconfigurant l'application selon un compte utilisateur spécifique. C'est extrêmement utile dans les workflows de télésanté, pour les patients comme pour le personnel, mais aussi pour tous les cas où un appareil est utilisé comme kiosque. Si Jamf peut préconfigurer les applications de cette façon, c'est grâce à sa prise en charge d'AppConfig. Cette puissante fonctionnalité de MDM permet de charger des réglages, des identifiants et plus encore, avec l'application. Livraison des applications, gestion des mises à jour et des réglages : tous ces atouts se combinent pour offrir une expérience utilisateur simplifiée et un accès direct à la plateforme WebEx.



**Nous sommes conscients que cela fait beaucoup à assimiler.**

Les possibilités sont immenses lorsque vous associez Cisco à Jamf, la référence pour gérer et sécuriser Apple en entreprise. Alors, essayez Jamf gratuitement et voyez par vous-même. Nous vous accompagnerons à chaque étape du processus.

**Demandez un essai** ou contactez votre distributeur Apple habituel pour commencer.