



Definitive Guide to Jamf and Cisco in the Enterprise



Cisco connects and secures end users to the networks and resources they need to succeed, regardless of where they are. Network infrastructure, security tools and end-user applications work together to establish a secure environment and support your organization. And in a world that is increasingly dispersed and reliant on mobile users and networks, having tools that secure networks and solutions that support productivity, collaboration and employee satisfaction is essential.

As the **dominant player in the enterprise network world**, it's entirely possible that Cisco is already your organization's go-to solution. Or perhaps you just started searching for the best technology stack for your Apple-focused organization. Regardless of where your organization falls in respect to its network systems, we're here to explain how Jamf and Cisco integrate and provide best-of-breed solutions that enhance your organization's network, security, device management, productivity and IT visibility.

Together, Jamf and Cisco make the most of your corporate IT investment. Through product integrations and our dedicated focus on Apple, your users will benefit from seamless and secure access to the resources that matter.

In this guide, we provide an overview of the Jamf-Cisco integrations that support your organization's Apple fleet.

Table of contents:

[Cisco ISE](#)

[Cisco SecureX](#)

[Fastlane+](#)

[DUO](#)

[Cisco DNA](#)

[WebEx](#)

Integrations

Cisco ISE

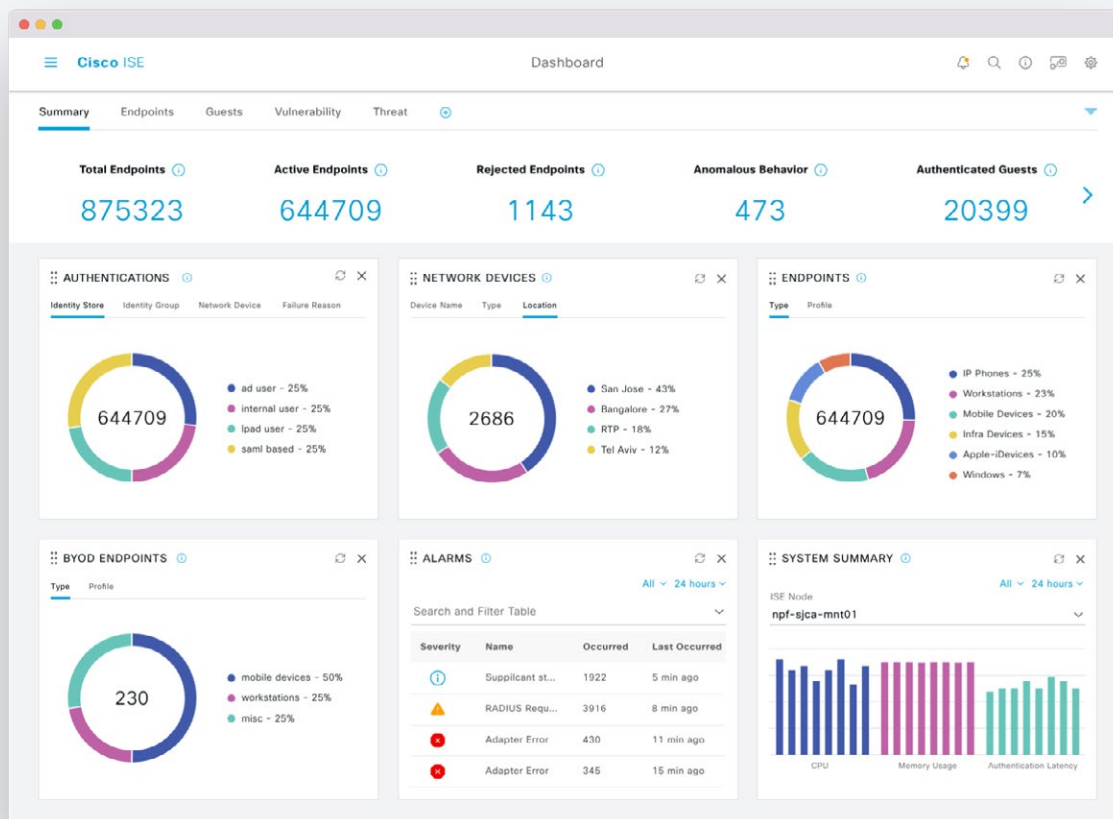
It starts with the network

Cisco Identity Services Engine (ISE) provides highly secure network access to users and devices with a zero-touch strategy. Gain visibility into what is happening in your network, such as who is connected, which applications are installed and running, and much more, and automate policy enforcement. When integrated with Jamf's device management capabilities, you can extend the power of Cisco ISE to identify, contain and remediate threats faster and more efficiently.

How? It's easy.

Network integration with Cisco ISE allows the service to communicate with Jamf Pro and verify that the computers and mobile devices on your network are compliant with your organization's standards. Once the data is collected from Jamf Pro, the service can determine the level of network access to grant to a computer or mobile device, provide messaging to end users and refer end users to enroll their computers and mobile devices to Jamf Pro, ensuring only compliant devices and users are accessing your network.

This integration also allows the network access management service to send remote commands to computers and mobile devices via Jamf Pro, including passcode lock and wipe commands, for continued support and security of your users and network.



Cisco SecureX

Device insights for increased visibility across all your tools

Device insights from Cisco SecureX unifies multiple device managers, endpoint detection and response, antivirus (AV) and other endpoint security products to consolidate the details those tools and solutions provide into a unified view within SecureX.

With device insights, you are able to keep track of device inventory counts and better understand the expanding and changing nature of your network. Furthermore, endpoint searching and reporting allows you to assess device security posture on employee-owned, contractor-owned and IoT/OT devices – without risking business disruption. Stop threats before problems occur!

Common IT-related concerns about inventory and asset management are just as easy to address as network concerns, given the single-pane-of-glass view into all your network-connected devices. By leveraging the link between Cisco and Jamf’s dashboards, admins can quickly jump from SecureX back into Jamf Pro to mitigate risks and perform triage on issues detected in Apple endpoints. This allows IT to pivot to remedial workflows, addressing issues as part of a single cohesive process.



User interface available in dark and light mode

Fastlane+

An intelligent network for Apple devices

Fastlane+, developed by Cisco and Apple, is a solution that significantly improves the experience of any Wi-Fi 6 capable Apple iOS/iPadOS devices that are connected to a Cisco Wireless Wi-Fi 6 network. By leveraging Wi-Fi 6's OFDMA technology, Fastlane+ provides users with an incredible voice and video streaming quality under even the most congested RF environments for clients running iOS 14 or higher. Fastlane+ enhances the existing Fastlane solution, optimizing iOS client roaming with adaptive 802.11r and allowing users to prioritize specific voice and video applications.

With Fastlane+, organizations identify which applications they want to prioritize on their network. After a network is configured to enable Cisco Fastlane+, organizations need to use an enterprise or mobile device management (MDM) solution, like Jamf, to configure it on the device level.

With Jamf Pro, organizations enforce the identified priority applications on each managed device, or across groups of devices, ensuring that when the network is congested, non-critical apps don't impact the performance of the apps that matter.



DUO

Enhanced endpoint security

Duo's Trusted Endpoints feature lets you define and manage trusted endpoints and grant secure access to your organization's applications with policies that verify systems using device certificates, application verification or management status. Duo helps organizations distinguish between unmanaged and managed endpoints accessing your browser-based applications.

With the Jamf Pro integration, Trusted Endpoints identifies which clients accessing the applications are managed and blocks access to various applications from unmanaged systems. Users authenticate to applications protected with Duo's browser-based prompt. Then, with managed device information obtained from Jamf via a nightly sync with read-only API, Duo matches device identifiers reported by the Device Health app.

The screenshot displays the Duo dashboard for Acme Corp. The interface includes a search bar, a navigation sidebar, and several data panels. The 'Users' panel shows 23 Bypass Users, 0 Locked Out users, and 491 Inactive users. The 'Endpoints' panel shows 661 Out of Date OS devices, a 6.7% increase in change over the last 7 days, 4.9k Up to Date devices, and 5.8k Total Endpoints. A list of metrics includes 195 Administrators, 4264 2FA Devices, 121 Groups, 13.9k New Trust Monitor Security Events (with 2.7k Priority Events), and 2.4k Remaining Telephony Credits. A bar chart shows 9.8k authentications over a 48-hour period. An authentication log entry shows a successful login for user 'belinda' at LotusSpa on a Mac OS X 10.15.7 device.

Dashboard

Search for users, groups, applications, or devices

Acme Corp | ID: 1234-5678-90 | Jewel Newport

Users

- 23 Bypass Users
- 0 Locked Out
- 491 Inactive

Endpoints

- 661 Out of Date OS
- 6.7% ↑ Change in the last 7 days
- 4.9k Up to Date
- 5.8k Total Endpoints

195 Administrators

4264 2FA Devices

121 Groups

13.9k New Trust Monitor Security Events

2.7k Priority Events

2.4k Remaining Telephony Credits

9.8k Authentications

In the last 48 hours, shown at every 30 minutes.

Authentication Log Last 10 attempts

Timestamp (PDT)	Result	User	Application	Access Device	Second Factor
12:15:46 PM AUG 16, 2021	✔ Granted Valid passcode	belinda	LotusSpa	Mac OS X 10.15.7 (19H1030) As reported by Device Health	Yubikey Passcode Location Unknown

What's New?

August 12th, 2021

Duo Universal Prompt

Duo Universal Prompt is now available for public preview. You can easily activate the new prompt for users with a single

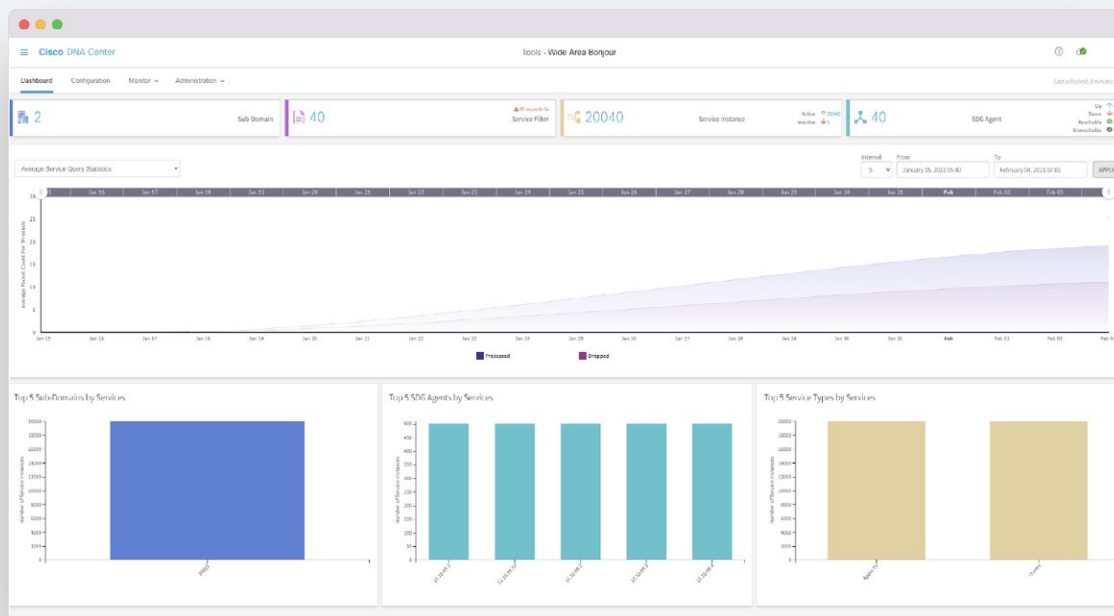


Cisco DNA

Adapt amazing Apple features for your network

Cisco Digital Network Architecture (Cisco DNA) has been able to simplify enterprise networks and make them more intuitive for customers. Cisco DNA Service for Bonjour solution enables mDNS service routing for Apple or industry standard-based devices. The Wide Area Bonjour capabilities support end-to-end Unicast-based service routing with enterprise-grade scale and security while maintaining consistent user experience at residential or best-in-class enterprise networks.

Schools with Apple devices on their network need a way to streamline the Apple device network capabilities in a scalable way to provide a customizable, personalized experience. The Cisco DNA solution supports collaboration, content sharing and IoT devices. Teachers can now share content and apps with their students and students can use a streaming technology like AirPlay to collaborate with each other, without issues typically seen in larger networks.

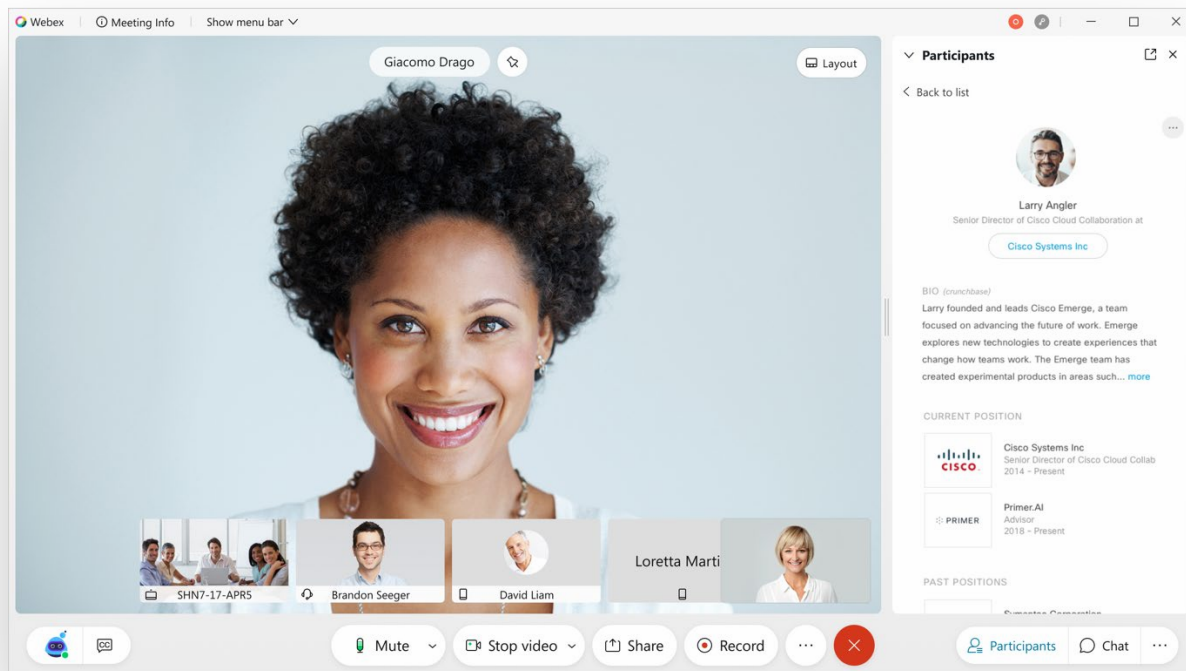


WebEx

Deployment and configuration

WebEx powers collaboration. From the basics of communication, like video and voice, to advanced features that let remote teams work seamlessly like whiteboarding and Augmented Reality (AR), WebEx supports any type of project.

With Jamf, WebEX empowers users to leverage these tools. This integration makes the solution available and configured for your organization's needs, in addition to ensuring that it is up to date on users' managed Mac and mobile devices. Jamf's proficiencies in [Application Lifecycle Management](#) make it simple to ensure the right apps and versions are always on a user's device. Going even further, Jamf can customize the experience of WebEx on iPad to be preconfigured with a specific user account. This is incredibly helpful with virtual telehealth workflows for patients and staff, and in other situations where a kiosk type device is required. Jamf's ability to preconfigure applications is based on our support of AppConfig, a powerful feature of MDMs to load settings, credentials and more alongside the app. This combination of app delivery, updating and settings management results in a simplified user experience where they can instantly benefit from the WebEx platform.



We know this might be a lot to take in.

And so much is possible when you pair Jamf — the standard in Apple Enterprise Management — with Cisco. So, try Jamf for free and see for yourself. We'll help you along the way.

[Request Trial](#) or contact your preferred Apple reseller to get started.