The Advanced Guide to Mac Management

The security landscape

Cybersecurity continues to improve.
According to PwC's recently-released 2023 Global Digital Trust Insights report, cybersecurity has improved in many ways since 2020: over 70% of 3,522 C-Suite leaders from a wide range of industries and global locations initiated improvements in cybersecurity in 2021.

We still have a long way to go.
38% of respondents believed they had completely mitigated risks related to enabling remote and hybrid work, for instance, while 48% believed they had moderately mitigated those risks. 35% reported complete mitigation of issues around swiftly accelerated cloud adoption.

However, **only three percent report that they have fully mitigated emerging cyber risks**. Only five percent reported that they were optimizing in all five aspects of the security workflow of identify, protect, detect, respond and recover.

Unfortunately, cybercriminals only need one way in to create havoc.
How can InfoSec and Mac administrators ensure that **all security protocols** are in place **across all areas** of the digital environment?

Only

38%

report that they have fully mitigated emerging cyber risks

Proper Mac management is secure Mac management

This 201 guide to Mac management, a follow-up to our Mac Management for Beginners e-book, discusses how managing macOS devices is the key to securing your Apple fleet. Proper management isn't the entire picture of the security landscape, but it's the foundation that all organizations must build from.

Read on for more detail on how proper management is security. We'll also cover the key capabilities, workflows and settings needed to securely manage your Mac fleet and cover all the bases.

PKI and push certificates

PKI certificates

A PKI certificate is a text file that contains identification data on machines, users and devices. Basically, it confirms the security of the computer and secures information going from one place to another with encryption.

In Jamf Pro, you can choose to use a built-in certificate authority (CA), integrate with a trusted third-party CA (DigiCert, Venafi, or Active Directory Certificate Services), or configure your own PKI if you have access to an external CA that supports the Simple Certificate Enrollment Protocol (SCEP). The CA can be used to issue certificates to both computers and mobile devices. When using Jamf Pro, the built-in CA certificate; revoke and renew, create a built-in certificate from a certificate signing request (CSR) and create a backup.

Certifications can be used for Single Sign-On (SSO), enrollment profiles, device management with the Jamf Binary, configuration profiles and more. Admins can deploy them manually through a web portal, through automation with a third party such as Jamf Connect, or through a direct certificate request: an automated process where the device communicates with the server via Jamf Pro.

Encryption with certificates not only secures all communication; it also allows for immediate revocation of access from people leaving the company or devices falling out of compliance.

Push certificates

A push certificate is an encrypted file generated by Apple that establishes trust between a third-party service like Jamf Pro and Apple Push Notification Service (APNs). A push certificate is created by Apple, but needs a third-party service, like Jamf, and APNs. They use an organization-owned Apple ID rather than a personal Apple ID.

Push certificates allow for the Jamf Pro server and APNs to communicate. APNs control info, specifically info from apps, sent to and from devices. Push notifications are how apps on devices receive communication.

As the file is an encrypted file generated by Apple, you can remotely uninstall an app based on this security information. Push certifications are valid for one year and must be renewed with the same Apple ID that created it initially.

How to find certificates

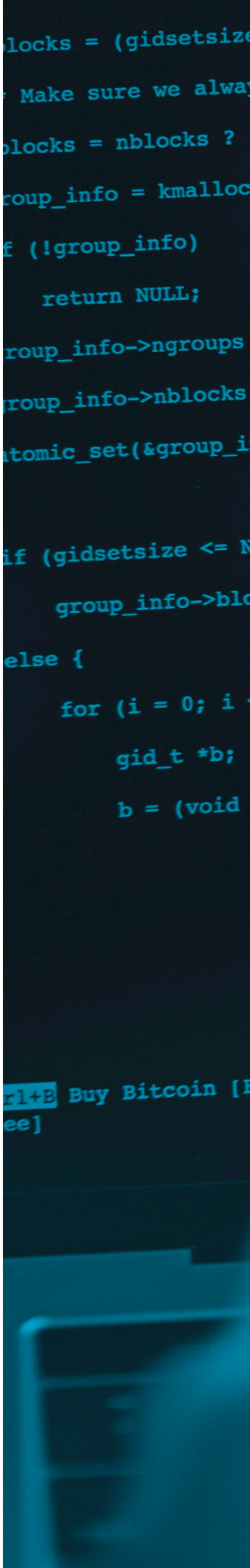
You can view a list of certificates by exporting to .csv, .txt., or XML files. Jamf Pro makes this process easier by walking an IT admin through the process to create a push certificate (.pem) and to upload it to Jamf Pro. You'll need a valid Jamf ID and Apple ID, and it's critical that Mac admins keep these certificates up-to-date. If they lapse, APNs will lose connection to your mobile device management (MDM) server/endpoints.

Conditional Access

Due to the new normal of remote work from homes, coffeeshops, or even on flights, companies can no longer create a network and protect devices and users via a firewall.

Conditional Access allows an organization to set parameters for securing an organization's data in multiple locations. It can gate access to organizational data such as email, OneDrive, Word and Excel— and Cloud Apps like Jamf Pro by evaluating the risk at that time.

Requiring a trusted device and a trusted user for access improves management and security, no matter where someone is working.



Organizational Macs are managed by Jamf and registered with Microsoft Intune through a cloud connector or manual connector. Jamf and Microsoft's strong partnership ensures that this works seamlessly: Jamf sends macOS device inventory to Intune. Intune evaluates compliance and generates a compliance report. Azure AD enforces access controls.

To learn more about creating a comprehensive compliance policy for Mac that keeps your devices, users and organizational data secure, please read Compliance Management for Beginners.

TeamViewer: remote Mac admin access

TeamViewer is a fast and secure solution for gaining access to computers and networks remotely. It establishes a remote screen-sharing connection between a Jamf Pro administrator and an end user's computer.

This improves security and compliance as admins can view, assess and solve problems quickly without any information lost in translation. And it speeds up problem-solving. When those problems impact security, speed really matters.

You'll need a TeamViewer integration configuration added to your Jamf Pro instance to access this capability.

Jamf API

The Jamf API is about making Jamf more accessible. It allows organizations to fit Jamf Pro into their tech stack, creating a cohesive system where Mac management is integrated. This powers interconnectivity between Jamf and other vendors and allows for integrations such as Jamf Protect/Jamf Connect, the Jamf School Parent App, the Jamf Teacher App, and more.

The token-based authentication scheme of the Jamf API hardens the security posture of devices interfacing with third-party applications and integrations. It's a RESTful interface, which means it follows secure software communication standards.

Workflow

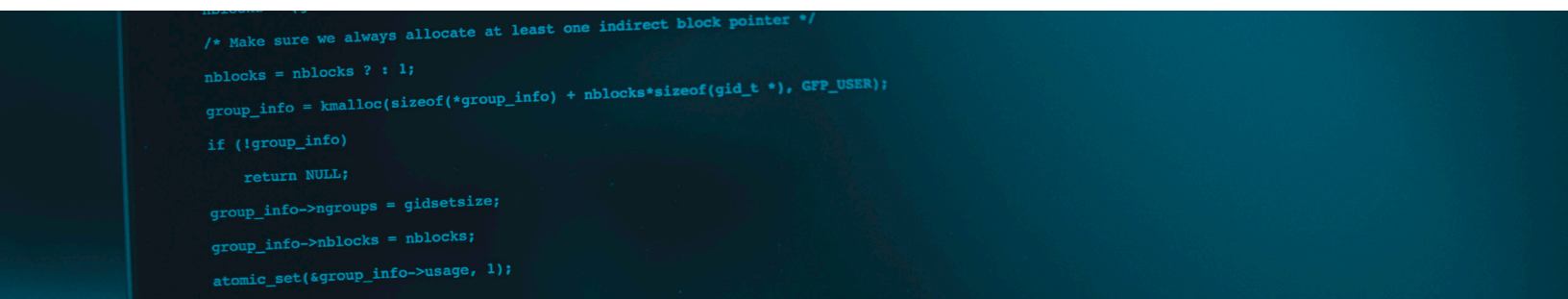
1. Using basic authentication, request a Bearer Token by sending a POST to `/v1/auth/token.`

2. You should receive a response that includes a token and an expiration date similar to the following example:

```
{
    "token": "eyJhbGciOiJIUzUxMiJ9...",
    "expires": "2022-01-24T21:35:20.373Z"
}
```

3. You can use the previously-generated token to make calls to any other Jamf Pro API endpoint by including it in a header using the format Authorization: `Bearer TOKEN VALUE.`

Integrations allow for a more holistic view of Jamf's capabilities, and a lock-tight connection with Jamf Protect, endpoint protection capabilities with network threat prevention for Mac. This allows admins to prevent macOS malware, to protect against specific events and to monitor endpoints and remediate issues quickly.



Webhooks

Webhooks allow a Mac admin to subscribe to a specific event on a Jamf Pro instance. When the event happens, an HTTP POST payload is sent to a specified URL. They allow admins to use real-time events from Jamf Pro to build custom workflows on-demand—using the programming language of their choice.

Webhooks support cybersecurity by keeping IT admins up-to-date on real-time events in their instances, sent as XML or JSON. And they can allow admins to create generic payloads like ComputerAdded (new computer enrolled), ComputerCheckin (check for tasks) or ComputerPatchPolicyCompleted (when a patch policy is completed).

Distribution points

Distribution points are servers used to host files for distribution to computers (and mobile devices). Packages, scripts and in-house apps and books can be distributed using a distribution point.

Jamf Pro supports file share distribution points and a cloud distribution point. Jamf will reach out to on-premises distribution points to find apps and deploy them to devices/users with file sharing. Admins can also distribute apps using Jamf's cloud-hosted distribution point: Jamf Cloud Distribution Service (JCDS).

Distribution points can be a weak spot in organizational security, as they are more often in the cloud with users located globally. Distributing files to Macs through an absolutely secure distribution point is critical.

How distribution points work with Jamf

By default, the first distribution point you add to Jamf Pro is the principal distribution point. All other distribution points depend on the first as the authoritative source for all files during replication. Distribution points guarantees that files will be sent to the correct device/user in the correct manner.

Scripting, config profiles and disk encryption: working together

Scripting

Automating common tasks increases security tenfold: removing human error in implementation as well as the chance that an admin will forget an important task. This can be done through scripting. Scripting can automate many tasks, and gives admins more control over their Mac applications.

Scripting is about practice and starting small. Have a task you'd like to automate? Use Jamf Nation and other Mac Admin boards to search for scripts that others have already created for that purpose.

Want to dive in with specific scripts and tasks? Read Automating common tasks with Apple scripting and Jamf.

Configuration profiles

One important way scripting can amplify and secure an admin's control is by implementing configuration profiles.

Configuration profiles are XML files (.mobileconfig) that provide an easy way to define settings and restrictions for devices and users. They typically use APNs. When creating a computer configuration profile, admins must specify the level at which to apply the profile—computer level or user level. Each level has a unique set of payloads and a few that are common to both.

Configuration profiles can enforce and enhance security in their own right by enforcing security protocols in passcodes, behavior and more.

Configuration profiles are built into Apple Configurator 2, Profile Manager and Jamf Pro— and can be deployed to devices and users with MDM enabled. There are two different ways to distribute a configuration profile: install it automatically (requires no interaction from the user) or make it available in Self Service.

Disk encryption

While scripting and configuration profiles are powerful tools, anything that can control the actions of a device must be secured absolutely. Disk encryption guarantees that information is secure behind a passcode. It encrypts code and scripts by moving them into an unreadable state that will be difficult to decipher. And it's built into Mac.

Disk encryption also allows Mac admins to manage and enable FileVault on computers. FileVault encodes info on Macs, preventing anyone from reading the information without a passcode.)

Extension attributes

Extension attributes are custom fields you can create to collect almost any type of inventory data from devices. You can use custom LDAP attributes to create extension attributes. And if you'd like, you can get even more advanced extension attributes with scripting.

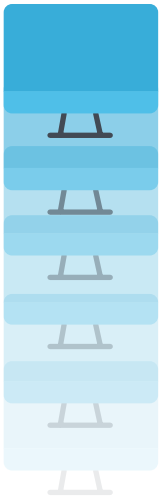
How to use them
Once the data from extension attributes is in the inventory record, admins can take action with Smart Groups with Jamf Pro: grouping devices and/or users into groups based on one or more inventory attributes. IT admins can not only manually create extension attributes to fit their needs but also leverage the templated Jamf Pro extension attributes for easy, efficient extension attribute creation.

Using extension attributes with Jamf Pro's Smart Groups can allow you to keep your fleet secure with group action on devices with any OS that needs updating and more. Implementing extension attributes will also provide a more cohesive understanding of the data in your instance, which allows for better views of what is out of compliance or weak points in the system.

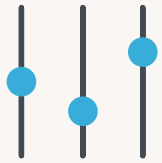
Mass actions

Another way to perform multiple tedious tasks on many computers simultaneously is mass actions. With Jamf Pro, admins can create mass actions on any Smart Group or static group, computer search results or lists of license usage matches. Mass actions can be anything. A few examples: remote commands, editing a side panel or emailing users.

This keeps environments more secure; whether managing five or 5,000 computers, mass actions ensures there is virtually no chance a device will be missed that might cause a security breach.



App management



As apps continue to be the most dominant part of the end-user experience, Mac application management is a vital element in managing and securing devices. From sourcing and hosting to updating and deploying, proper app management is critical in securing an Apple fleet while also supporting end-user productivity.

Many of the most-used apps today are not in the Mac App Store. App Installers provides a better way for Mac admins to automatically source, host, update, and deploy apps to their computers or users. Out-of-date apps are a major security concern.

That's why Jamf offers ways to stay on top of app updates:

App Installers
App Installers is a curated collection of Jamf-managed and Jamf-provided installer packages that streamline deployment and offers a streamlined alternative to complex workflows required to patch third party apps.

To ensure security, they also validate the integrity of patch definitions before allowing deployment. Once verified, the new app version will be deployed automatically to all compatible Macs.

These are the packages that Jamf sources, re-packages and hosts. This Jamf App Catalog is a collection of software titles including a list of 1,000+ third-party macOS software titles supported in Jamf Pro.

App Installers must be in a smart computer group in Jamf Pro. If a target computer in a smart group has the software title installed, the App Installer deploys the update when a new version is released.

Patch policy workflows
Most Mac admins are familiar with the manual process of deploying patch policies. Jamf offers workflows for these actions, which take care of bug fixes— vital for network security as bugs in third-party apps are one of the most-used ways of breaking into otherwise secure environments.

A complete understanding of your app environment will provide you with an understanding of what apps are out of date on what computers. This process is automated with App Installers, and can run in the background.

Title Editor
Title Editor is a Jamf-hosted service that extends patch management by providing custom software titles, overriding existing patch definitions and the ability to create custom patch definitions.

Jamf security solutions for Mac

While it's clear that diligent management of Mac devices is vital to proper security, it's important to remember that device management is the foundation for security. Using security-specific tools on top of that firm foundation is the last piece in the security puzzle. For a basic overview, please read Mac Endpoint Protection for Beginners.

Jamf Protect endpoint protection

Jamf Protect goes beyond a simple antivirus tool for malware. It's a complete endpoint security solution with behavior-based detection that anticipates and recognizes behaviors often used in attacks.

You'll also discover the importance of other systems of security, including Identity and access management, threat prevention and remediation, content filtering, and Zero Trust Network Access (ZTNA) in keeping users, devices and organizational data secure.

How Jamf can help

Jamf Pro

For a strong and secure foundation, try Jamf Pro — the standard in Apple device management. You can learn more and request a trial directly from us, or contact your preferred reseller to get started.

Security beyond device management

Read our report on the state of Apple security in the enterprise, which surveyed 1,500 IT and InfoSec professionals. It includes current device usage and approaches, challenges to device security and the future state of endpoint security.

Trusted Access

Trusted Access is Jamf's solution to security beyond management. Trusted Access is a unique workflow that brings together device management, user identity and endpoint security to help organizations create a work experience that users love and a secure workplace that organizations trust.

Ensuring that only trusted users on enrolled, safe devices can access company data, Trusted Access with Jamf dramatically increases the security of your modern workplace while streamlining work for your users — regardless of where work happens.

Learn more about Jamf's state-of-the-art, Mac-first security offerings to see how we can help you continue to manage and protect your Mac fleet!

At Jamf.com/solutions, discover more about:

- **Identity and access management**
- **Content filtering and safe internet**
- **Endpoint protection**
- **Zero Trust Network Access (ZTNA)**
- **Threat prevention and remediation**
- **Security visibility and compliance**

> And if you're ready to dive in to managing and security your Macs with Jamf, **request a free trial today!**

Source:
1. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html