jamf

The IT Checklist for Mac Compliance

Compliance isn't just about meeting legal requirements. It also increases security, reduces risk and builds trust.

Why does Mac compliance matter?

Most organizations, regardless of size or industry, must comply with some form of compliance regulations, especially when handling sensitive data.

A compliance benchmark in IT security is a set of standards used to measure an organization's adherence to regulations and requirements and provides best practices for protecting sensitive data.

For example, CIS Controls and Benchmarks are widely adopted across industries as a foundational layer of security best practices. While not tied to any single regulation, they often serve as a baseline on which organizations build additional industry-specific or region-specific compliance measures, such as those required by GDPR or HIPAA.

Organizations must adhere to these benchmarks to decrease security risk, build customer trust and avoid penalties. In fact, failure to comply with relevant regulations can result in hefty fines, legal action and reputational damage. Regularly tracking and meeting these benchmarks helps companies stay secure and competitive in the digital world.

The art of maintaining Mac security for IT admins

Part of why IT admins love Apple is that the Mac has incredible built-in security features.

Mac computers are, by their very nature, more stable and efficient than other devices. And with the right tools, IT can enforce powerful, flexible Apple-specific management and security measures without hampering Apple's excellent UI experience. When you combine a world-class MDM solution with Apple's Declarative Device Management (DDM) protocol, you can ensure that company data, employee data and networks are protected.

Regulatory compliance for Macs:
What to consider

There is a great deal to consider when focusing on compliance within your organization.

Your organization will probably have multiple compliance standards to meet. This will ensure corporate and employee data stays secure. You'll need to enforce these as well as industry and governmental benchmarks.

Just how many regulations are there?

Each industry and region has its own regulations and best practices, and some overlap. A small sample from around the world:

ISO

ISO 27701 certification ensures proper handling of PII (Personally Identifiable Information) in healthcare across the globe

DORA regulations address financial regulation in the EU

CIS benchmarks from the Center for Internet Security offer prescriptive configuration recommendations to keep organizations safe

NIS2 requirements ensure adherence to EU-wide legislation on cybersecurity

The German IT Security Acts 1.0 and 2.0 (das IT-Sicherheitsgesetz 1.0 und 2.0) regulate IT security with their own compliance requirements

Cyber Essentials+ defines minimum cyber security standards for all organizations in the UK

These are certainly a lot of complex regulations to track and enforce!

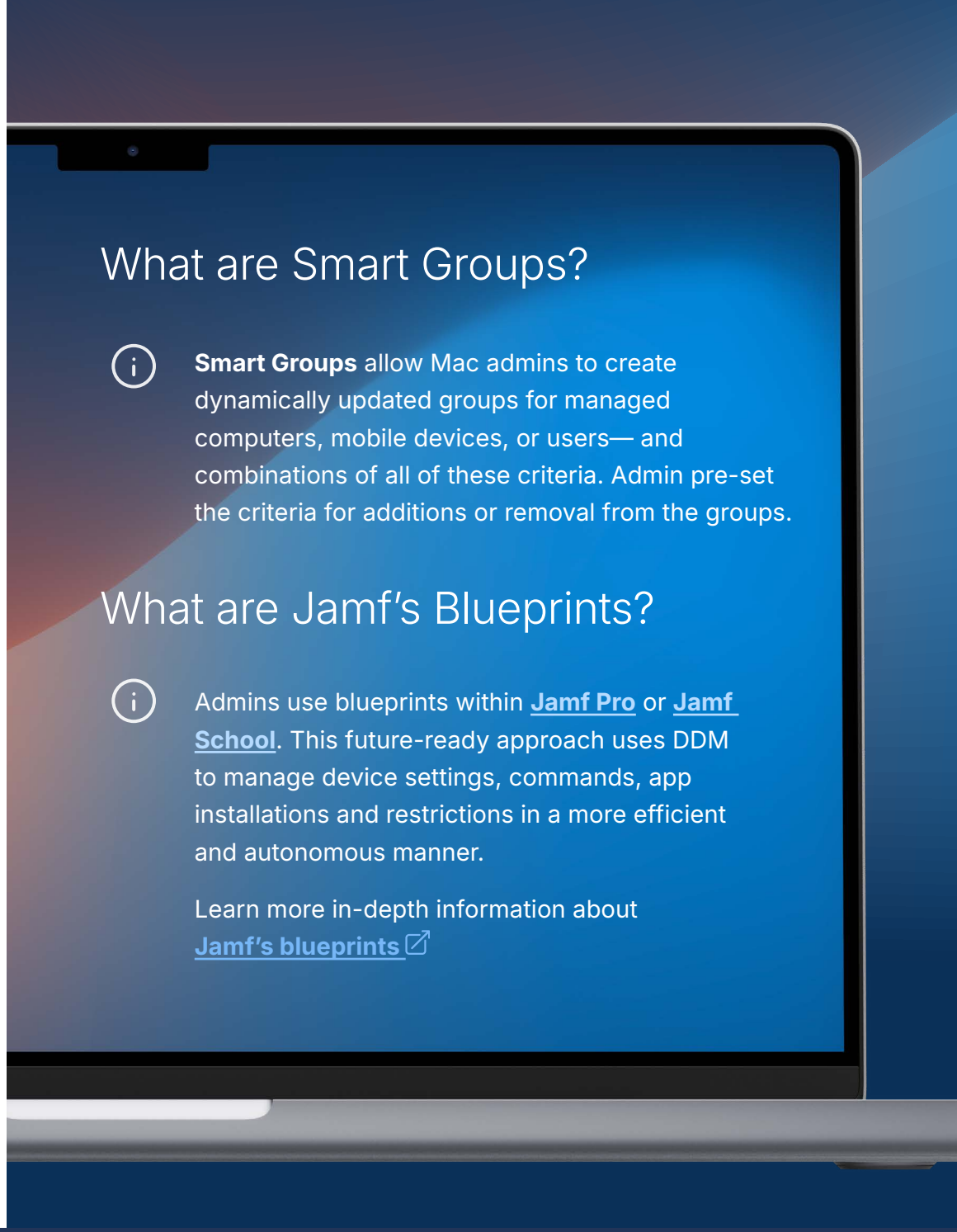
Let's say that you persevere; you do the research and determine which regulations apply to your organization and device environment. Now, thanks to your world-class MDM and your own thorough QA process you can implement an automated way of setting and continuously validating compliance.

With device management you have:

- **Well-crafted configuration profiles, compliance declarations and blueprints**
- **Smart Groups set up for dynamic profile and command assignments**
- **Automation that saves time and ensures immediate adherence to compliance on the device level**

You can log out triumphantly, perhaps indulging in a long-delayed nap.

Except...



...In compliance, everything always changes.

As the internet, IT, business practices and laws change so must your compliance configurations. The point of compliance is to keep businesses safe and running smoothly. Keeping up with emerging security and IT issues is part of the process.

This requires:

- ✓ **Regular compliance audits and regulatory reviews**
- ✓ **Speedy OS updates**
- ✓ **Proactive monitoring of cyber threats**
- ✓ **Adherence to changing compliance regulations**
- ✓ **Swift response to staff and policy changes that affect who has access to what data**

If this all sounds really overwhelming, that's because it is.

Enter the Mac compliance checklist and Jamf.

By following a structured checklist, IT can streamline compliance processes and stay ahead of evolving regulations. The best way to ensure you don't lose track of anything is a thorough checklist that contains detailed, specific steps to ensure that you have the right security configurations, monitoring and enforcement in place.

And don't forget the use of top-notch solutions that help to track, monitor, enforce and update all these areas.

Preparation phase

- ✓ **Create user accounts and profiles.**
- ✓ **Define organizational policies and permissions with decision-makers in your organization.**
- ✓ **Define outside compliance regulations based on which industry or governmental regulations your organization must follow.**
- ✓ **Ensure hardware and software compatibility with all tools you'll be using.**

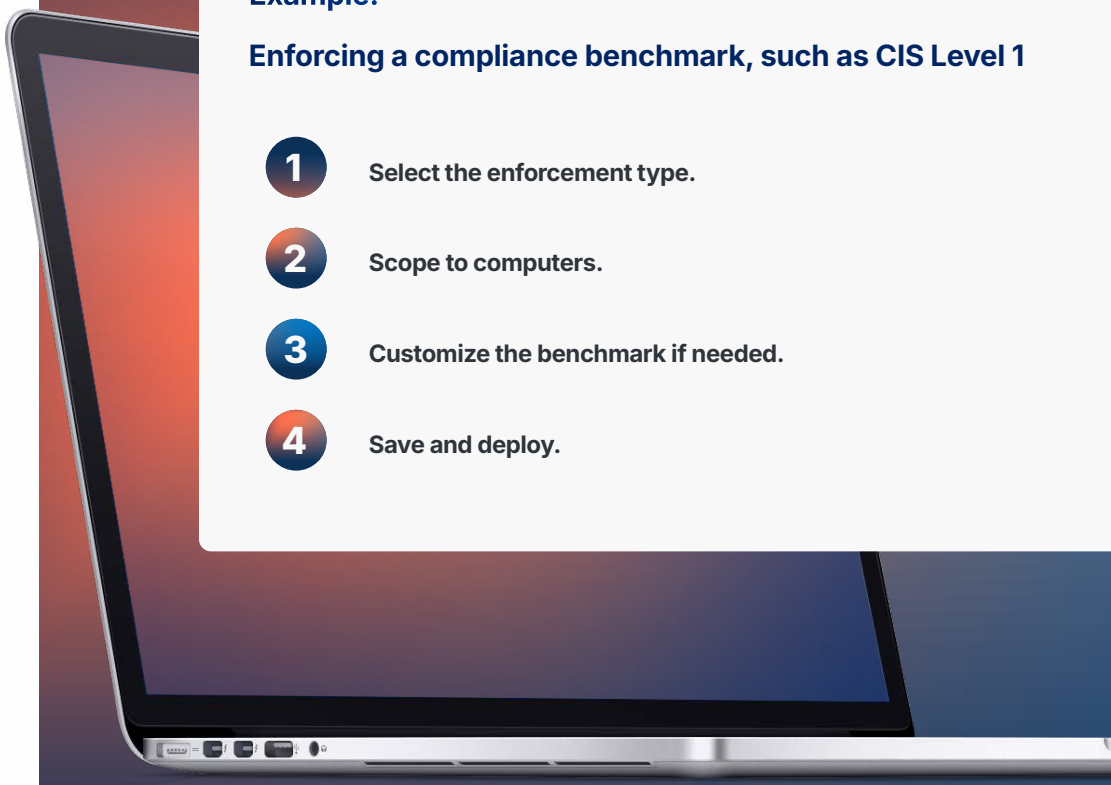
What is the compliance benchmarks feature?

Built into Jamf Pro, compliance benchmarks allow IT to define, audit and enforce compliance.

The feature:

- **Decreases time an IT admin needs to audit and enforce a compliance benchmark in their device fleet from weeks to minutes.**
- **Hides the complexity of the compliance standards, rules and configuration controls behind a simple and easy to understand UI and workflow.**
- **Increases customer device fleet security posture.**

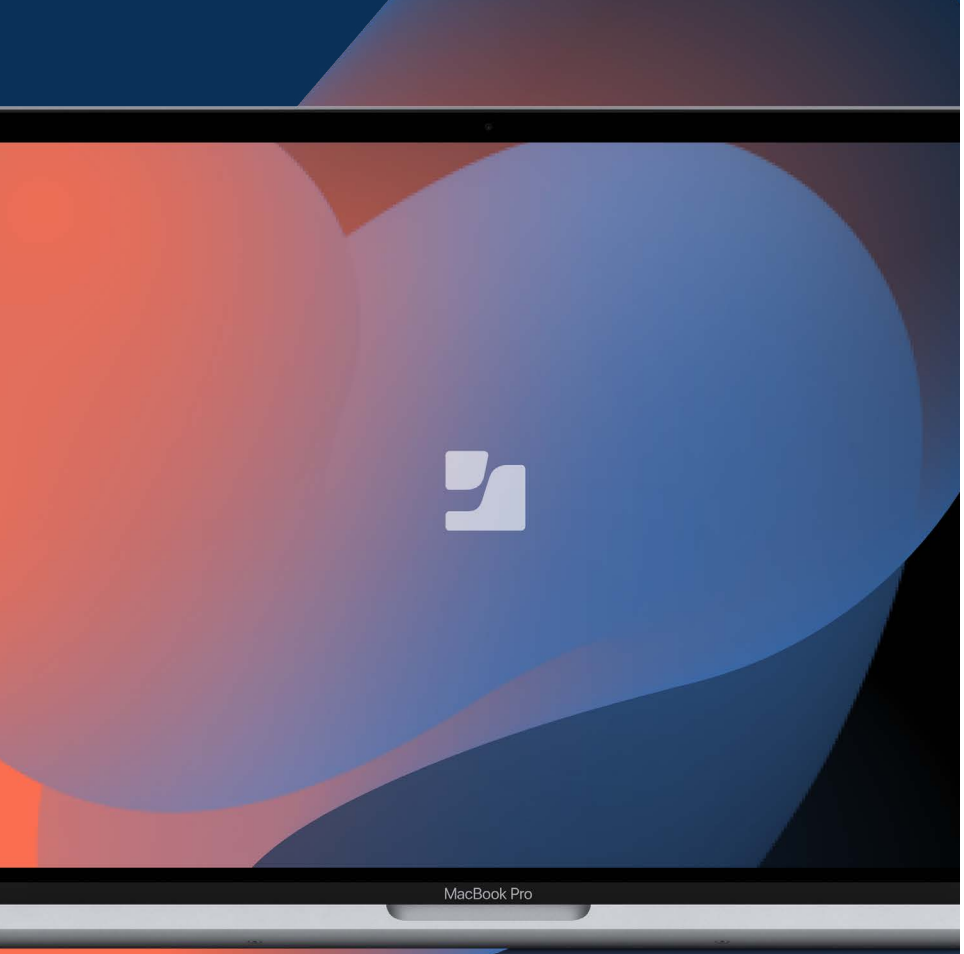
Compliance benchmarks create all of this automatically and include profiles, policies, scripts, extension attributes and more. They create Jamf Pro configurations that change and maintain device configurations to ensure compliance with the selected benchmark.



Example:

Enforcing a compliance benchmark, such as CIS Level 1

1. **Select the enforcement type.**
2. **Scope to computers.**
3. **Customize the benchmark if needed.**
4. **Save and deploy.**



Compliance benchmarks were built on the macOS Security Compliance Project (mSCP). It's a joint effort of federal operational IT security staff from the National Institute of Standards and Technology (NIST), National Aeronautics and Space Administration (NASA), Defense Information Systems Agency (DISA) and Los Alamos National Laboratory (LANL).

Continued maintenance and monitoring

The compliance benchmarks dashboard displays all created benchmarks and their statuses. More detailed views display all devices' compliance per compliance rule (e.g. require a minimum password length) to allow admins a closer look.

Watch a compliance benchmarks demo:

Setup and configuration

Use automated provisioning with MDM and DDM to ensure that each device has exactly what it needs for each user, and that the apps and access settings are proactively updated at the device level.

- ✓ **Use Jamf's compliance benchmarks to simplify and speed up your workflow by using Jamf-created requirements based on common benchmarks, such as CIS level 1 or 2. Admins can also create custom benchmarks.**
- ✓ **Use one of six quick-start templates within the Jamf blueprints window or create your own. This saves time and increases security with passcode policy settings, service configuration files settings and background task management.**
- ✓ **Install essential apps and updates using a combination of Self Service+ (which allows certain user groups to access and download apps and resources specific to their roles) and Smart Groups.**
- ✓ **Configure security settings (FileVault, Gatekeeper, etc.).**

Testing

- ✓ **Verify functionality of apps and system features.**
- ✓ **Conduct security audits; Jamf Protect keeps audit logs that can aid IT with this job.**
- ✓ **Consider rolling out these changes to a smaller group of employees first who can function as on-the-job testers.**

Start out strong

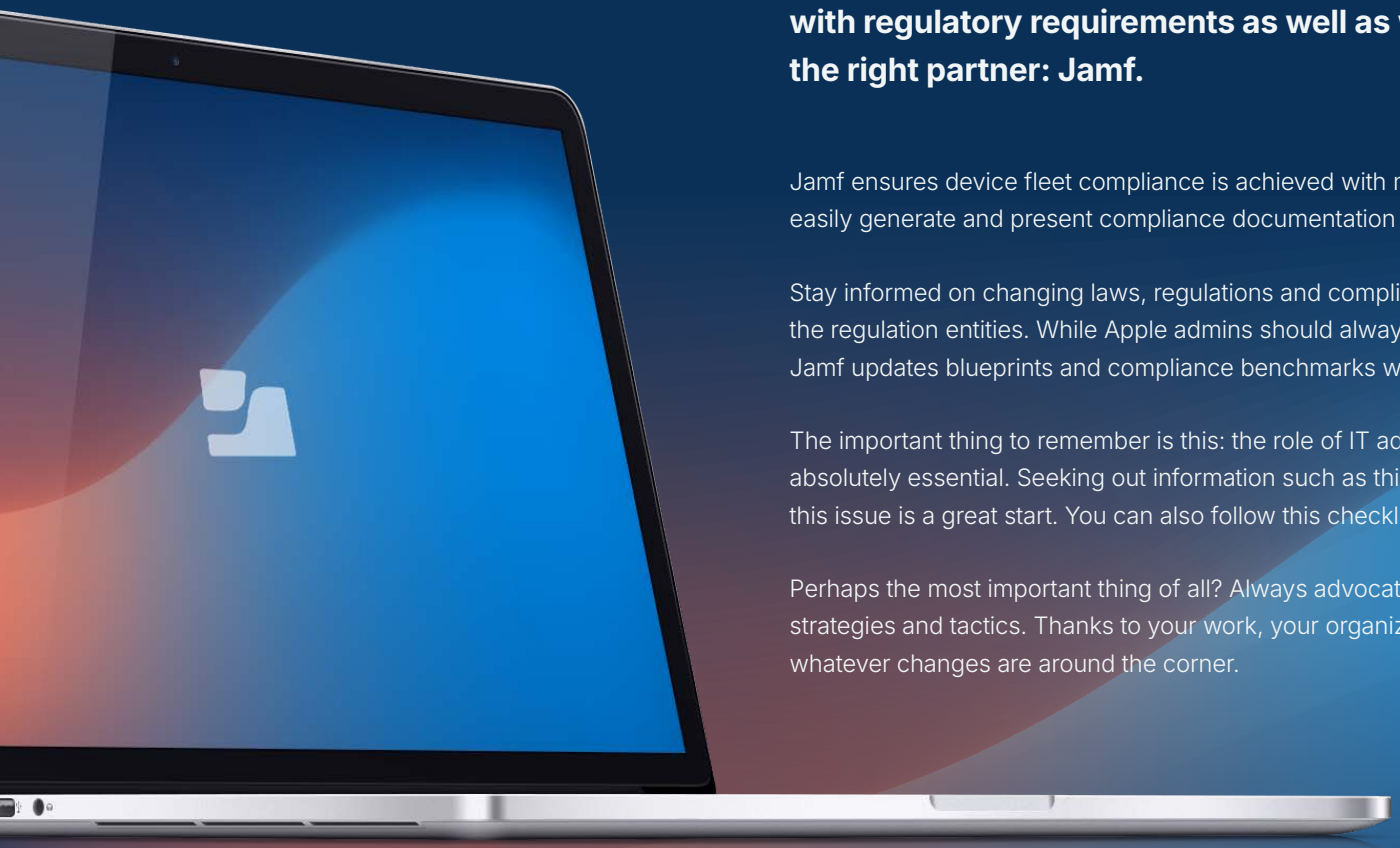
- ✓ **Provide clear instructions to users.**
- ✓ **Schedule an onboarding session for questions and troubleshooting.**
- ✓ **Ensure you are correctly set up for automated updates on compliance settings through Jamf; it will take the legwork out of remaining on top of new developments for many key compliance protocols.**

What is Self Service+?

Self Service+ is an end-user portal for macOS. It allows users to access content and updates that have been preconfigured in Jamf Pro. In Self Service+ users can:

1. **View the security status of their devices.**
2. **Browse, search, and install apps from the App Store and third parties, configuration profiles, and books.**
3. **Perform identity management tasks such as changing passwords.**

Best practices and future considerations



You can ensure that your device fleet is securely configured and compliant with regulatory requirements as well as with internally defined policies with the right partner: Jamf.

Jamf ensures device fleet compliance is achieved with minimal IT admin effort. Security teams can also easily generate and present compliance documentation and status to auditors.

Stay informed on changing laws, regulations and compliance standards by following announcements from the regulation entities. While Apple admins should always have an idea of what's ahead in compliance, Jamf updates blueprints and compliance benchmarks when these details change.

The important thing to remember is this: the role of IT admins in future-proofing compliance efforts is absolutely essential. Seeking out information such as this e-book to better understand the importance of this issue is a great start. You can also follow this checklist.

Perhaps the most important thing of all? Always advocate for faster and more reliable compliance strategies and tactics. Thanks to your work, your organization will be future-proofed and ready for whatever changes are around the corner.