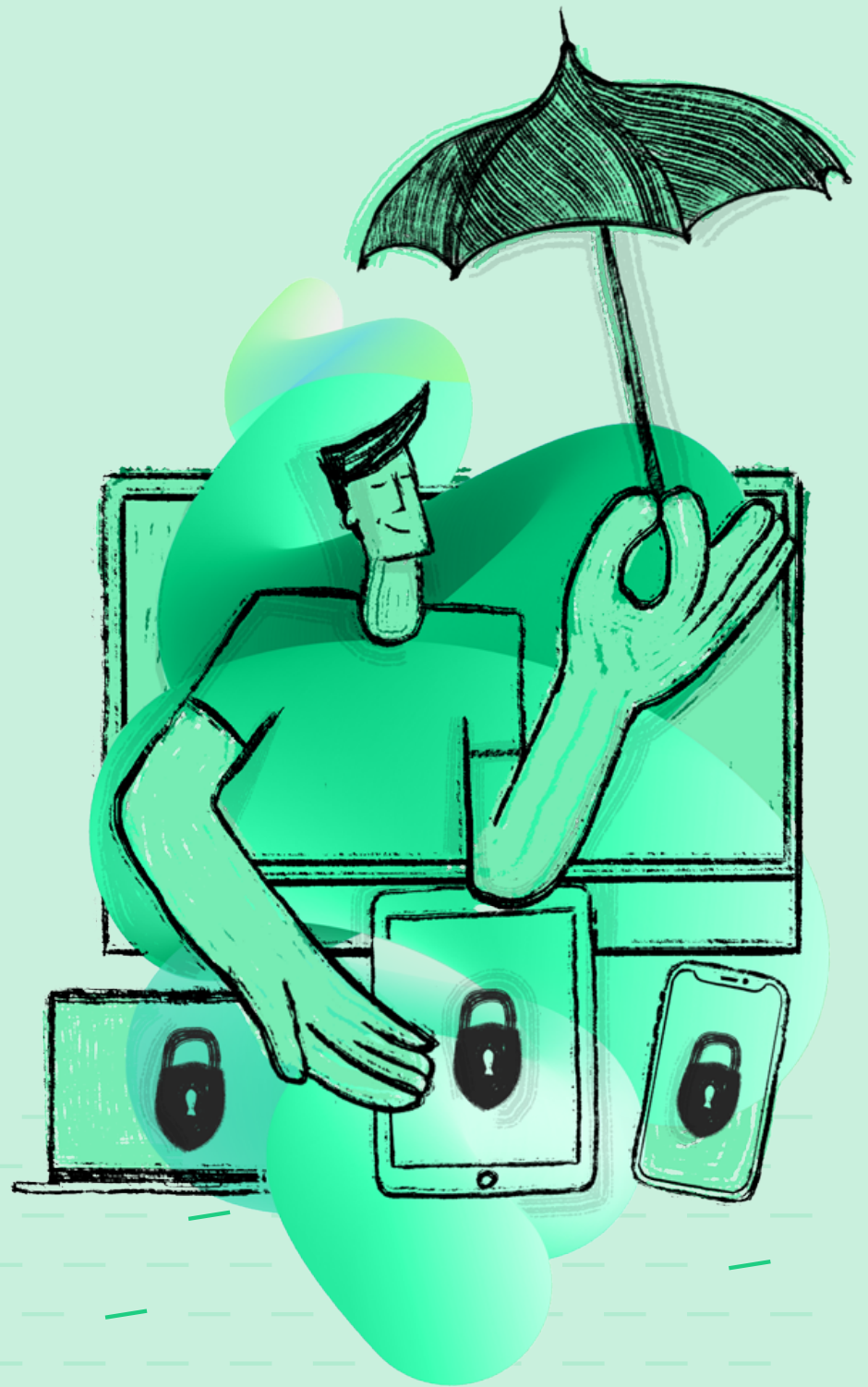




Device Compliance

MSP Deployment Kit





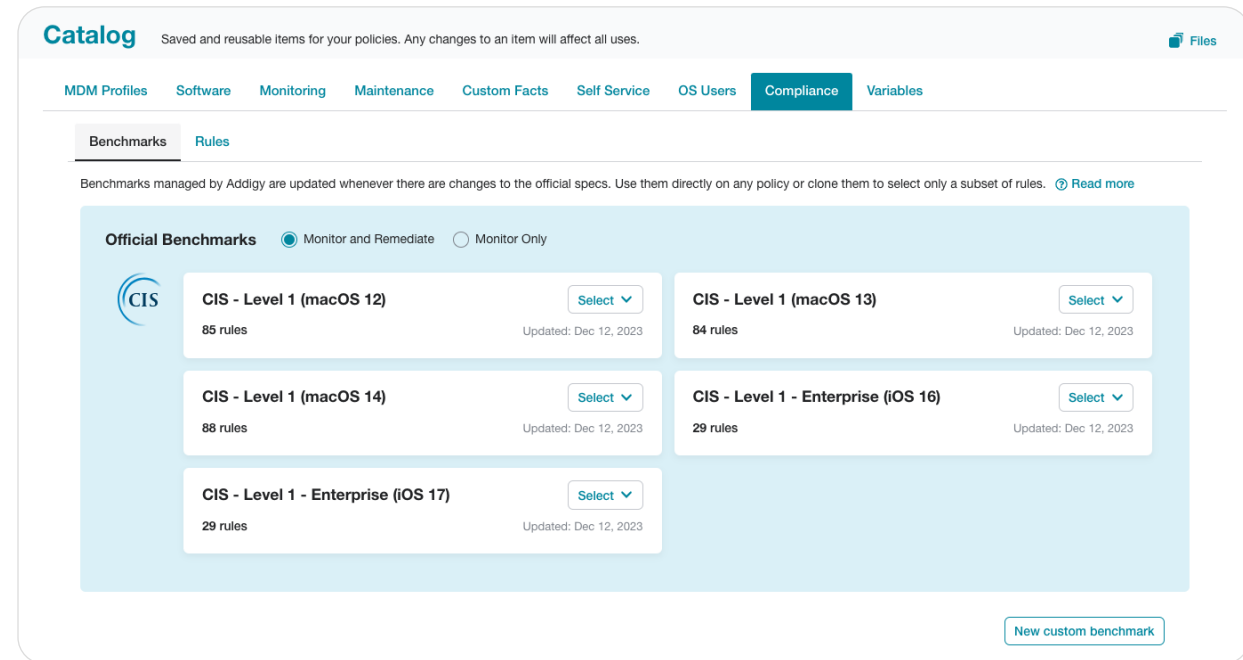
Increase Revenue

Addigy Device Compliance with pre-built benchmarks is a highly valuable tool.

Consider providing remediation to your clients as a one-time project or as a recurring fee so clients appreciate the value you're providing.

Add Value and Deploy with Confidence

Deploying Addigy Device Compliance allows you to quickly secure all of your clients' macOS, iOS, and iPadOS devices. Device Compliance greatly reduces the security risk of an organization, and implementing it with Addigy saves hours of time. However, it requires more effort than simply activating the feature within Addigy. It's also essential to provide a great client experience when deploying.



This kit is designed to support your Addigy Device Compliance deployment plan with clear communications so you can inform your clients of the changes, add value and revenue, and provide them with the resources they need to keep their employees secure and productive.

Inside this deployment kit, you'll find guidance, customizable templates, and reference materials you can use to build your program, communicate details, and support your clients throughout the process.

Planning > Communication > Resources



Eat Your Own Cooking

We recommend implementing this entire plan first internally with your Apple device users so you feel comfortable talking about it with your clients.

Planning

CIS, NIST, or Custom?

As part of Addigy's **Device Compliance**, we're maintaining a set of **pre-built benchmarks** to enable you to test your devices easily for CIS and NIST compliance. These are available in the catalog alongside your custom benchmarks in the **Compliance tab** and can be assigned directly to multiple policies.

Decide which benchmarks you'll use and the policies you'll apply them to. Consider splitting iOS and iPadOS devices into separate child policies from the macOS devices to make applying the benchmarks to the appropriate device types easier. CIS is a great starting point if you're unsure about which benchmarks to apply.

Remember that you can always clone a set of benchmarks and remove or add rules to suit each of your client's unique needs.

Benchmark Settings

CIS - Level 1 - Enterprise (iOS 17)

OS: iOS 17 (all versions)

Managed by Addigy

[About pre-built benchmarks](#)

29 Rules

- > 1. Ensure iCloud Backup is set to Disabled
- > 2. Disable iCloud Keychain Sync
- > 3. Ensure Managed Apps Storing Data in iCloud is Set to Disabled
- > 4. Ensure Allow iCloud Documents and Data is set to Disabled
- > 5. Ensure Treat AirDrop as unmanaged destination is set to Enabled
- > 6. Ensure Allow documents from managed sources in unmanaged destinations is set to Disabled
- > 7. Ensure Allow documents from unmanaged sources in managed destinations is set to Disabled
- > 8. Ensure Force Apple Watch wrist detection is set to Enabled
- > 9. Ensure Require Touch ID / Face ID authentication before AutoFill is set to Enabled
- > 10. Disable Sending Diagnostic and Usage Data to Apple

Close

Need only a subset of rules? [Create clone](#)

[Assign to policies...](#)



Clear Communication

Clear communication will set you apart from your competition. Leverage multiple channels (emails, meetings, videos, PDFs, and so forth) to reach the widest audience. And don't be afraid to repeat your message.

Listening is also essential. We love hearing from our customers, and we rely on you to share feedback from your clients.

[Please send us feedback.](#)

Monitor Only

Enable the Official Benchmarks as "Monitor Only" to evaluate the current device states. Do this for each of your clients. Note this is for macOS only. iOS and iPadOS do not allow for monitoring only.

Review the results internally

From the Addigy Devices page, create a new table view with the "Compliant" device fact to review the results and see if there are any concerns. You can also directly export several types of [compliance reports](#). Are some clients already compliant? Are any clients significantly out of compliance?

Share the results with your clients

Review the results with your clients and share the value of remediation to meet and enforce compliance. Compliance remediation is the process of recognizing problems and creating a plan to correct and prevent those problems from occurring again.

The Addigy Device Compliance for macOS, iOS, and iPadOS is a highly valuable tool. Depending on your current client relationship, you may decide to provide remediation at no additional cost, a one-time fee, or an ongoing monthly fee. You may also choose to charge differently for remediation on iOS and iPadOS versus macOS.

Deploy

Upon written approval from each client:

- 1 • Agree on the Remediation Pilot Program members
 - 2 • Set the Full Deployment Date
 - 3 • Share the Communication plan
-



Communication

Communication at key phases is critical to your success. Clear Communication will help create interest, support a successful launch, and encourage engagement. In the following pages, you'll find templates for email communication throughout these phases.

Pre-Sales One

SUBJECT: We've generated a Security Compliance Report for your Apple Devices

Hi, [CLIENT],

We've recently developed a security compliance report for your Apple devices. Your organization's cyber security is a top priority and this compliance report can help us identify and address possible holes in your cybersecurity framework. This report is based on [Apple's macOS Security Compliance Project](#) and extends to iOS and iPadOS devices. I'd love to share it with you. Here's my online calendar to book a time.

Thanks,
SIGNATURE

Pre-Sales Two

SUBJECT: Reduce Risk with Security Compliance for Your Apple Devices

Hi, CLIENT,

Thanks for your time today discussing our newly developed Apple device security compliance report. With your approval (ATTACH QUOTE or LINK HERE), we can schedule a time to start the remediation process, which will look like this:

- Define up to X number of macOS, iOS, and iPadOS devices (maximum of 10% of total fleet for each device type) for the Remediation Pilot Program.
- Set the Remediation Pilot Program Date and share the Communication Plan.
- Review and make any necessary changes to the benchmarks and communication.
- Set a Full Deployment date and share the Communication Plan.
- Full Deployment and sleep easier at night.

Thanks,
SIGNATURE





Got Questions?



Ben Greiner
Apple Champion
& Growth Advisor
ben.greiner@addigy.com

Book a Meeting

calendly.com/ben-addigy/30min

Resources

- [Addigy Pre-built Compliance Benchmarks](#)
- [Addigy Compliance](#)
- [Simplify Compliance and Enhance Security with Addigy](#)
- [On-Demand Demo: Addigy Compliance & Conditional Access](#)

Client Communication: Pre-Launch | Build Awareness

No one likes surprises, so help your clients feel comfortable by providing them with transparent and open messaging for their team. Ask them to let everyone know that changes are coming and they are essential. Use this with your Pilot Program Members, then refine it for the Full Deployment.

SUBJECT: Device Compliance Coming Next Week

Hi, Team,

Next Tuesday (INSERT DATE and TIME), we'll roll out our new Device Compliance initiative for company-owned Macs, iPhones, and iPads. This deployment will ensure that our devices are secure and help prevent us from becoming victims of cybercrime.

We don't anticipate you'll notice any changes to the day-to-day function of your devices. However, if you experience any disruptions, please contact (INSERT MSP NAME) for assistance: MSP CONTACT INFO.

Thanks,
SIGNATURE

Client Communication: Post-Launch | Reminder

Ask your client to remind their team of the changes and value you provide. Use this with your Remediation Pilot Program Members, then refine it for Full Deployment.

SUBJECT: Device Compliance is Here

Hi, Team,

This is a reminder that we've completed the deployment of our new Device Compliance initiative. This initiative is built to help protect us from cybercrime. We don't anticipate that you'll notice any changes, but if you do, please contact (MSP NAME) immediately for assistance: MSP CONTACT INFO.

Thanks,
SIGNATURE

