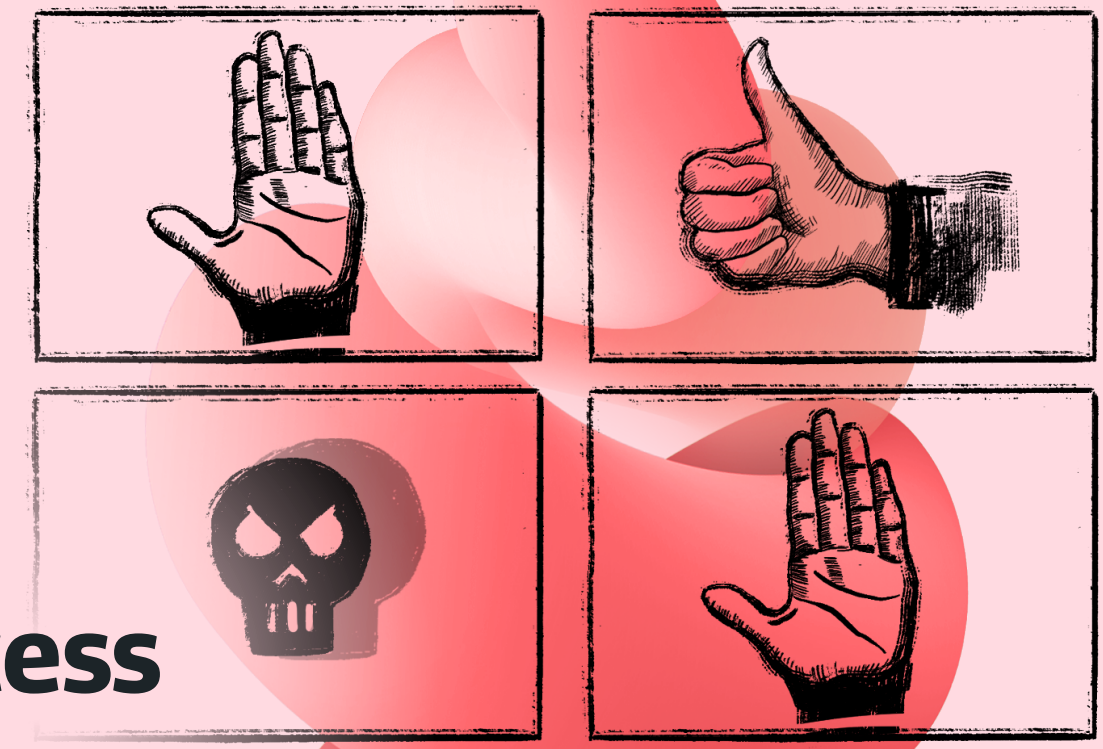
Addigy™

Microsoft Conditional Access

MSP Deployment Kit



Secure Devices and Deliver Peace of Mind

Increase Revenue

Microsoft Conditional Access with Addigy is a valuable tool. It is highly recommended that you provide this service to your clients as a one-time project and a recurring fee so that they appreciate the value you're providing.

Contact your Customer Success Manager within your Addigy portal to discuss pricing for more than two Microsoft Conditional Access connections.

Conditional access is a fundamental layer of protection for any organization. If a device doesn't meet specific conditions, it won't gain access to company resources because it could be a security risk.

Deploying Microsoft Conditional Access with Addigy means more than simply activating the feature. It also requires communicating its value and providing a great client experience.

This kit is designed to help you inform your clients of the new workflow, educate them on the benefits of a more secure environment, and position you as a thought leader in the Apple, Microsoft — and security and compliance space.

What is Microsoft Conditional Access?

Microsoft Conditional Access is a way to ensure that a device meets specific conditions before it's granted access to company resources.

Ensuring end users access to organizational data from a trusted device is crucial to many security best practices. Combining Microsoft Conditional Access (to validate the user) and Addigy (to secure the device) allows Apple admins to verify that access to corporate assets is secure.

Addigy Device Compliance is a key part of this solution. Each time a device checks in, Addigy runs an audit to confirm compliance and sends this information to Microsoft. Addigy is one of only a few **device compliance partners** authorized to enhance the Microsoft Intune experience.

Using Addigy and Microsoft, organizations can ensure that only managed and compliant Apple devices can access their Microsoft email, Microsoft 365 services, and any web or desktop apps authenticated with Microsoft credentials.

Preparation

Before introducing this solution to your clients, first become familiar with **Addigy Device Compliance** and **Microsoft Conditional Access** within your own organization.

With Addigy's Device Compliance, you can apply **prebuilt device compliance benchmarks** to enforce CIS or NIST compliance, or build custom benchmarks to suit your unique needs.

You'll then leverage your Addigy Device Compliance settings to tell Microsoft if your devices meet the conditions for access to company resources.

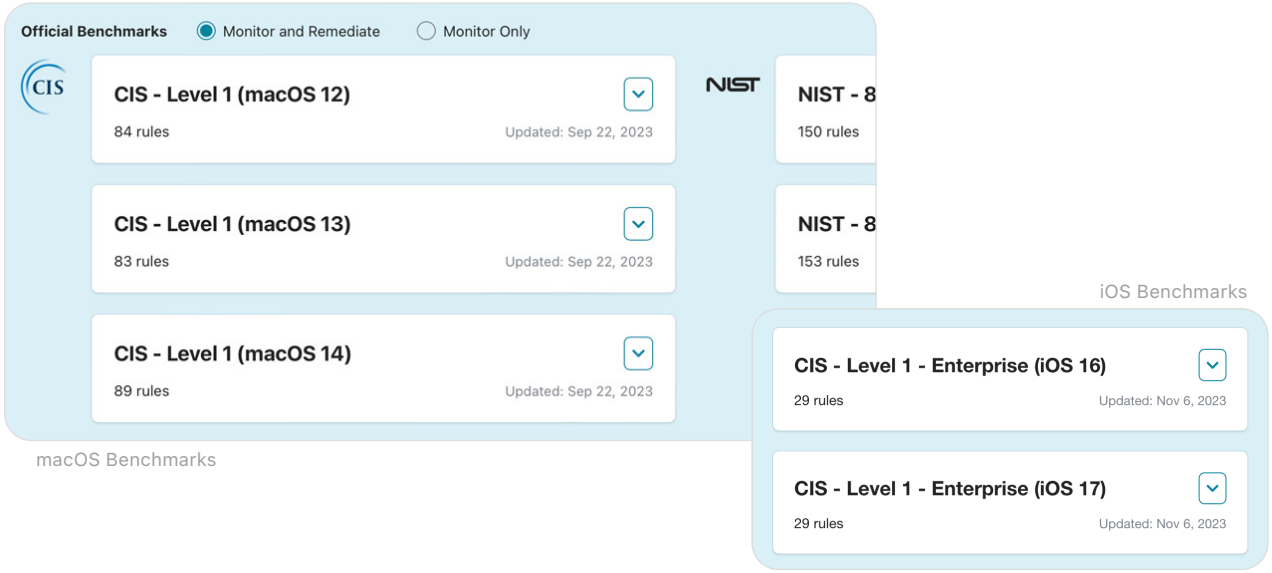
Eat Your Own Cooking

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

We strongly encourage you to use the report-only modes for Addigy Device Compliance and Microsoft Conditional Access to test and monitor usage before enforcing.

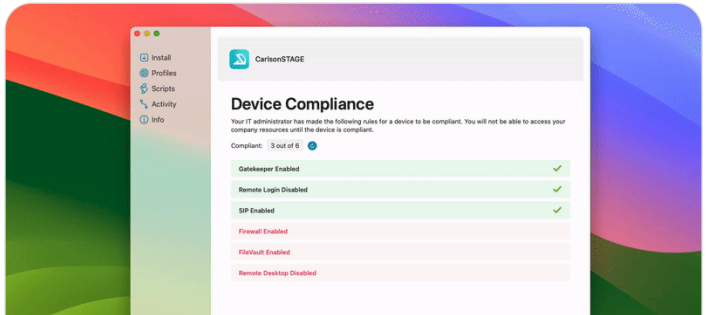
Requirements

- **Microsoft Entra ID P1** or **365 Business Premium** licenses.
- Macs running macOS 11 Big Sur or newer
- iPhones/iPads running iOS/iPadOS 15 or newer



Deployment Strategy

With any change to processes or workflows, it's important to thoroughly test the new configurations before rolling out en masse. To that end, it's recommended to follow a limited testing strategy to ensure that Conditional Access is working as intended in your clients' unique environments. This also enables you to provide a tangible demo to the clients, showcasing how the new feature will interact with their day-to-day experience.



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 (for you and us)! We love hearing from our customers, and we rely on you to share feedback from your clients.

Please send us feedback.

Our recommended strategy follows this plan:

1- **Identify the Compliance Benchmarks to be enforced for each client.**
Each client will likely have different requirements that define what makes a device compliant. You'll want to ensure the benchmarks accurately reflect the client's needs. The standard CIS or NIST benchmarks (prebuilt in Addigy) may be the perfect solution for many clients. But there may be cases where some rules must be omitted or changed. In those cases, you can create **Custom Benchmarks** with rules not covered by the preconfigured benchmarks.

2- **Pilot a subset of devices to be included in the initial wave of testing.**
Once you've decided on the initial benchmarks to be enforced, work with your client to assign a batch of their devices to pilot and test the new feature. We recommend aiming for a small subset, about 10 percent, of the overall fleet to be used for the initial pilot.

3- **Test thoroughly and ask for feedback.**
During the initial pilot, contact your client and ask for feedback. This will allow you to identify issues, help them feel involved in the process, and allow you to educate them on the new rules being implemented.

4- **After testing, develop a full rollout plan with clear start and end dates.**
Once the initial pilot program is successful and you're aligned with your client's goals, it's time to begin a rollout plan for the rest of their fleet. A tiered approach over time is a good approach, allowing you to push 10 to 15 percent of their total device count each week for a set amount of time until total adoption. With enough client buy-in, you may opt for a total rollout across the entire device base.

Whatever option you and your client decide on, communicate the plan and agree on the project's target dates. Target dates provide a tangible timeline for both of you, and these dates can always be adjusted as needed.

5- **Following the full rollout, check in with your client.**
The final piece may be one of the most important. Checking in with your client following the full rollout will allow you to address any issues that may have cropped up and reinforce trust between you and your client. You're their partner in improving overall security, and good partners communicate regularly and effectively.

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 communication throughout these phases.

Email communications may not be enough. Consider hosting a Lunch and Learn to demonstrate what will be required to gain access to company resources. Record how everyone with an Apple device must launch Addigy Self-Service to register their device with Microsoft.

Communication templates for Client Decision Makers:

Pre-Sales One

Subject: Reduce Risk with Microsoft Conditional Access for Apple Devices

Hi, [CLIENT],

I want to ensure you know about a new way to improve security and reduce risk on your Apple devices using Microsoft Conditional Access.

Microsoft Conditional Access is a way to ensure that specific conditions are met before a device is granted access to company resources.

Ensuring end users access organizational data from a trusted device is crucial to many security best practices. I'd love to hear what you think about this. Please use my online calendar to book a time to discuss.

Thanks,
[SIGNATURE]

Pre-Sales Two

Subject: Protect Corporate Data with Microsoft Conditional Access for Apple Devices

Hi, [CLIENT],

Thank you for taking the time to discuss plans for rolling out Microsoft Conditional Access for Apple Devices. Once you approve the quote [LINK TO QUOTE OR ATTACH TO EMAIL], we can start the Pilot Program, which will follow this workflow:

1- Define devices for the Pilot Program.
2- Set a date for the Pilot Program communication and deployment.
3- Review the Device Compliance Benchmarks used for Conditional Access and adjust as needed.
4- Set a deployment date for full rollout to all devices and share a Communication Plan with end-users.
5- Deploy Microsoft Conditional Access to all Apple devices and enjoy improved security.

Thanks,
[SIGNATURE]

Addigy

Got Questions?

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

Book a Meeting

calendly.com/ben-addigy/30min

Resources

- Addigy Launches One-Click Compliance and Conditional Access for macOS Devices
- On-Demand Webinar: Next-Gen Conditional Access For Your Apple Devices
- Executive Order on Improving the Nation's Cybersecurity
- Microsoft 365 + the NIST cybersecurity framework

Client Communication: Pre-Launch | Build Awareness

Because Microsoft Conditional Access can directly affect the end-user experience, you must provide clear communication to the end-users. Encourage your clients to let everyone on their team know that changes are coming and are essential to reducing risk. Use these communications with your Pilot Program Members, then refine them for the Full Deployment.

Subject: Security Changes for Devices Accessing Office 365

Hello,

Next Tuesday (INSERT DATE and TIME), we will enforce **Microsoft Conditional Access** to improve the security of our Office 365 data.

This means that if your device (personal or company-owned) does not satisfy the compliance rules for our organization, your device will be prevented from accessing company resources at Microsoft 365.

If you experience an interruption on your device related to accessing Microsoft 365 resources, please contact (INSERT MSP NAME) for assistance: MSP CONTACT INFO.

Thanks,
[SIGNATURE]