CyberQP

How MSPs can Implement Compliance-Mandated Access Management Controls

E-BOOK

Table of Contents

Introduction

Due to changing compliance framework requirements for both privileged administrator and end user accounts under NIST and CMMC, CyberQP has created a complete guide to help you address each type of identity, how these changes impact you, and how your Managed Service Provider (MSP) can prepare to align with best practices.

We'll outline the updates to **NIST SP 800-63's** recommendation and **32 CFR Part 170, CMMC rule**, the US Department of Defense's final addition to the Cybersecurity Maturity Model Certification (CMMC) framework.

How to Secure Your Admin Accounts Under CMMC with Privileged Access Management

On October 2024, the Department of Defense published the final version of the CMMC program's rules. According to the Federal Register, these rules will take effect on December 16th, 2024, after the government finalizes the pre-existing DFARS clauses. Following initial implementation, the United States will begin ramping up enforcement and rollout of CMMC standards. One year after initial implementation, the government will require all contractors to meet NIST SP 800-171 r3's 110 cybersecurity requirements and achieve CMMC Maturity Level 2 and pass a CMMC Third-Party Assessment Organization (C3PAO)'s audit. Two years after implementation, the DoD hopes to require CMMC Level 3 for all contracts.

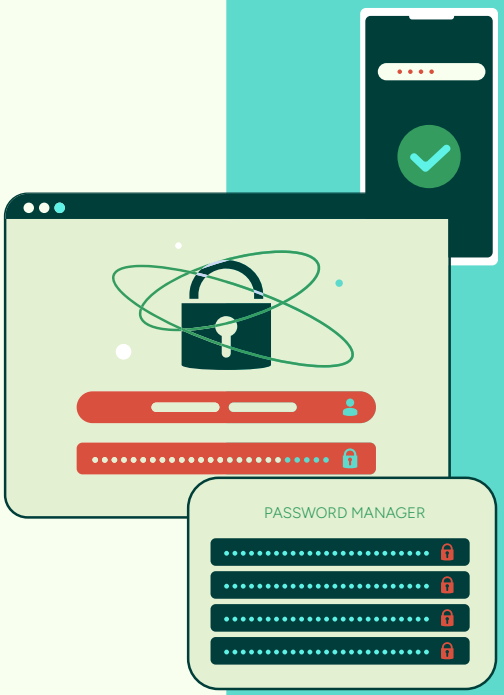
How These Changes Impact Your Privileged Accounts

Under the new guidelines, best practices call for MSPs to have the least amount of active admin accounts they need to reduce their security risks. Ideally, they would want to have "authenticators" (accounts, credentials, physical keys or badges according to NIST SP 800-171 r3, 03.05.12) with unique identifiers for technicians. For example, an admin account might be named after the technician it belongs to. Moreover, NIST requires under security controls (SP 800-171 r3, 03.05.01 and 03.05.12) that admin access be temporary when possible, requiring Just-in-Time access and that individuals re-verify their access when doing work that requires elevated privileges.

While NIST and CMMC do note that "the use of long passwords or passphrases may obviate the need to periodically change authenticators," that's not enough. These practices mean your technicians don't need standing administrator access for their day-to-day work, and that you need to show how admin access was assigned and why it was assigned. That's where unique, named Just-in-Time administrator accounts come in.

Seeing is Compromising: Protecting Your Admin Accounts in the Real World

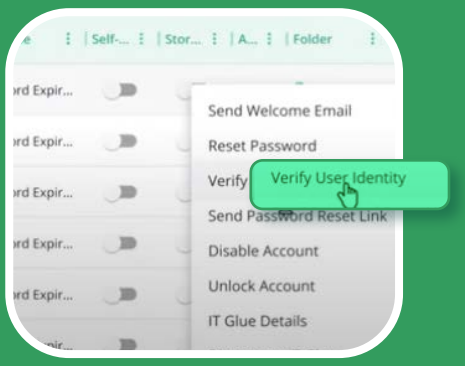
While these compliance best practices are important to consider in your MSP's day-to-day operations, there are other real-world factors to consider when considering how often you should be rotating or refreshing your privileged account credentials. While other NIST guidelines may not require you to regularly rotate admin passwords, when a technician can see and use an admin credential, they can be potentially considered an insider threat. Thus, when offboarding a technician, you may want to rotate any admin credentials that they had access to.

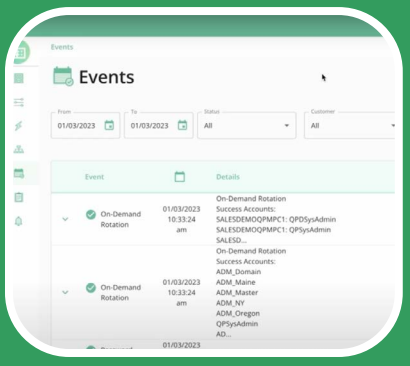


Examples of CMMC 2.0 Security Controls That Privileged Access Management Should Support:

Access Control (AC): Privileged Access Management solutions will help you limit access to sensitive information, keeping the number of security risks as low as possible and minimzing your attack surfaces.

Identification and Authentication (IA): This requirement calls for security measures to safeguard CUI and only grant access to authorize users, which specifically calls for identity verification before granting access to an organization's digital environments or devices. This control also specifically requires MFA for local and network access to admin accounts, which Privileged Access Management can provide.





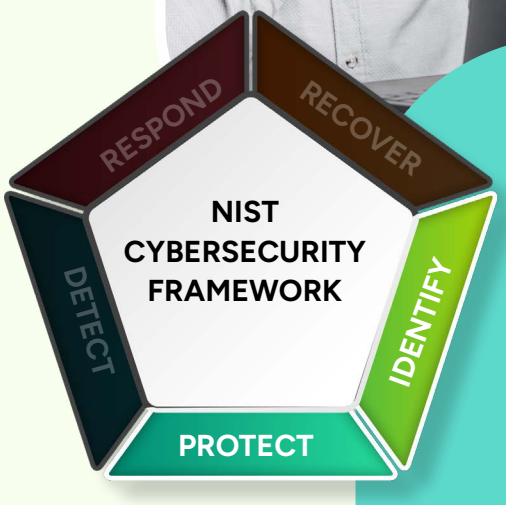
Security Assessment (CA): As a proactive security solution, Privileged Access Management can support this control, which requires an organization to regularly review their security programs and measures to ensure they're properly securing their data and complying with best practices.

Protecting Your Customer Identities Under NIST 800-63

What is NIST 800-63?

NIST's Special Publication (SP) 800-63 offers guidelines to help organizations manage and secure their digital identities, including how they can reduce their risks, how they can create and implement secure credentials and authenticator solutions, and outlines a "risk-based process to select assurance levels."

The changes outlined in this guide impact the "Identify" and "Protect" mappings the NIST framework. "Identify" helps organizations identify what they need to protect, assess vulnerabilities that could compromise sensitive assets, and focus their cybersecurity on mitigating relevant threats and risks, while "Protect" pertains to Identity Management, and following the Principle of Least Privilege, or limiting access to critical assets to authorized users, devices or processes.



The Latest Updates to NIST's 2025 Password Guidelines

Recently, the National Institute of Standards and Technology (NIST) released new updates to their best practices and compliance requirements, including their 800-63 guidelines surrounding password security.

In previous years, NIST's password guidelines prescribed securing all digital accounts with complex passwords or passphrases, leading to those infamous and ubiquitous requirements in every account creation menu (must include a certain minimum of uppercase and lower case characters, numbers, special characters, etc.).

So how do the agency's latest changes in 2025 impact an IT professional's day-to-day workflow and how corporate employees secure their data?

Eliminate Reused Credentials with Simpler Passwords

With these updates, NIST has acknowledged that their previous complexity requirements for passwords has led to users struggling to keep pace reusing passwords across different accounts, and making all of their accounts less secure by giving threat actors one password that can compromise multiple digital resources.

While NIST 800-63 previously required passwords to be a minimum of eight characters, the newest guidelines now call for passwords to be **twelve to sixteen characters**.

Because NIST observed that requiring users to change passwords every 60 to 90 days was contributing to an increase in reused passwords, they have also

Because NIST observed that requiring users to change passwords every 60 to 90 days was contributing to an increase in reused passwords, they have also retracted their guidelines around password expiration, and recommend only changing passwords in the event of a compromise.

HOWEVER: If a technician views or uses a credential, that credential may potentially be compromised. After all, in major incidents such as the Chimera breach, IT technicians can pose an insider threat to their employers, and technicians that do not follow best practices by copying and pasting admin passwords, screenshotting or deliberately saving their passwords and exfiltrating them poses major risks to any credentials a technician touches. In order to stay truly secure, MSPs need to create a Moving Target Defense by regularly rotating any passwords that a technician uses in their regular workflows and manually activating a rotation when a technician offboards.

Please note that NIST's requirements, while prevalent, are recommending the minimum level of security you should provide to your customers, and other compliance frameworks, such as PCI-DSS and the Federal Information and Security Management Act (FISMA) recommend regular password expiration and rotations for end users.

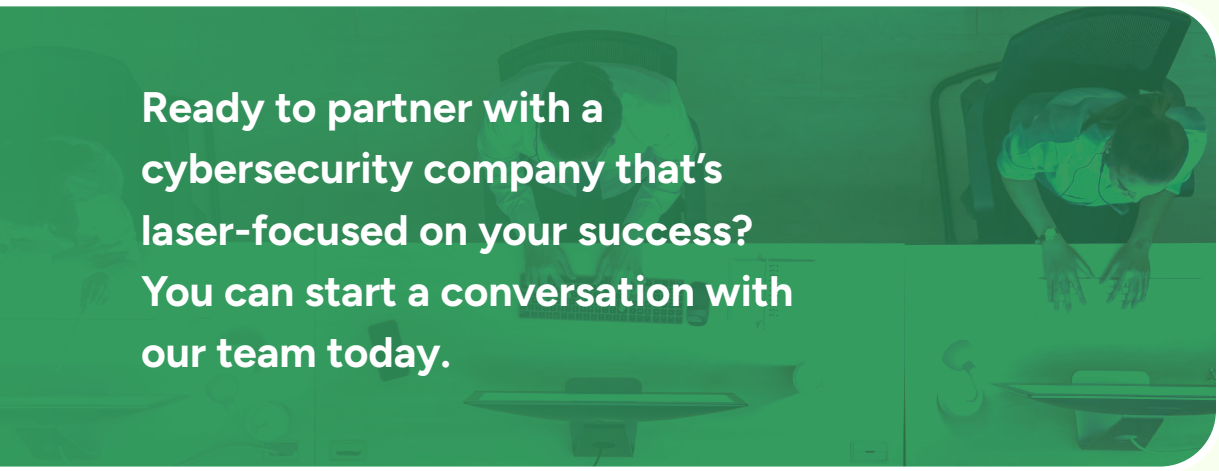
Conclusion

Conclusion

Today's IT professionals are a key part of helping any organization prepare for changing best practices or aligning with new compliance frameworks. By working in lockstep with cybersecurity experts, organizations can proactively enhance their security posture and mitigate potential security risks.

At CyberQP, we're prepared to help you implement security measures that will better prepare you to secure your help desk and your end users, such as Passwordless Just-in-Time Access, which helps address risks associated with compromised credentials – or Customer Workforce Verification to combat phishing and impersonation attempts.

We're also focused on helping our channel partners align with compliance frameworks. We run a dedicated InfoSec and Compliance team that runs penetration tests and threat modeling on all of our major releases and ensures we comply with best practices. Our solution is built securely, and we simplify the evaluation process during compliance or security audits with a dedicated Trust Center hosting all of our compliance mapping, and by not storing, transmitting, or processing CUI.



Ready to partner with a cybersecurity company that's laser-focused on your success? You can start a conversation with our team today.

Works Cited

Department of Defense. "Cybersecurity Maturity Model Certification (CMMC) Program, 32 CFR Part 170." Federal Register. Last modified October 15, 2024. https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program.

"CMMC Frequently Asked Questions." United States Department of Defense (DoD). https://dodcio.defense.gov/Portals/0/Documents/CMMC/CMMC-FAQs.pdf.

Doherty, Meghan D., Aaron S. Ralph, Brian E. Finch, Toghrul Shukurlu, and Aleksey Dabbs. "The Department of Defense Issues Final Rule Establishing CMMC 2.0." Pillsbury Law. Last modified October 25, 2024. JD Supra. https://www.pillsburylaw.com/en/news-and-insights/final-rule-cmmc.html.

Fenton, James L., Michael E. Garcia, and Paul A. Grassi. "NIST Special Publication 800-63-3: Digital Identity Guidelines." National Institute of Standards and Technology (NIST). Last modified June 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

"NIST Special Publication 800-63, Revision 4." National Institute of Standards and Technology (NIST). Last modified August 28, 2024. https://pages.nist.gov/800-63-4/sp800-63b.html.

"NIST Drops Password Complexity, Mandatory Reset Rules." Dark Reading, August 28, 2024. https://www.darkreading.com/identity-access-management-security/nist-drops-password-complexity-mandatory-reset-rules.

CyberQP redefines help desk security through privileged access management, help desk verification, and user privilege elevation. We empower MSPs and IT professionals to eliminate standing privilege risks, enforce compliance, and streamline operations. Committed to "Empowering Access, Redefining Privilege," CyberQP protects accounts, credentials, and identity verification with innovative, efficient solutions. Learn more: https://cyberqp.com/product-tours/