CMMC 2.0: A MANUFACTURER'S GUIDE TO ACCESS CONTROL AND AUTHENTICATION

How to secure access and meet CMMC 2.0 compliance without slowing users down

imprivata® | MANUFACTURINGDIVE

Custom content for Imprivata by studioID

CMMC 2.0 is here

Cybersecurity Maturity Model Certification (CMMC) 2.0 is now in effect. This framework raises the bar for security and is necessary to compete for valuable contracts, like those with the Department of Defense.

While stronger security is a clear benefit, compliance also paves the way for a more modern approach. One of the most impactful areas to focus on is **access control and authentication**, where security and productivity intersect.

This playbook explores how manufacturers can implement critical elements for CMMC 2.0 compliance — even on legacy technology — while keeping access simple and quick for busy frontline workers.

> **“You’ve got to secure their factory floor without disrupting operations. Compliance is critical — but so is keeping production moving.”**
>
> *— Chaitanya Yinti, VP of Product Management, Imprivata*

What comes next?

CMMC 2.0 requires manufacturers to control access to sensitive systems and verify user identities to prevent unauthorized access.

These requirements fall under two key areas:

- **Access control (AC):** ensuring only authorized users can access specific systems, devices, and data
- **Identification and authentication (IA):** verifying user identities before granting access to systems

Together, these controls form the foundation of a broader framework known as **identity and access management (IAM)**, which helps ensure that only the right people, using trusted devices, can access critical systems. Sean Ryan, Senior Product Marketing Manager at Imprivata, emphasized, "Cyberattacks often involve breached credentials or insider threats. Knowing who's accessing what – and being able to control and track it – is a critical first step toward compliance and stronger security."

For manufacturers, adopting this framework means:

- Eliminating shared logins and weak authentication practices
- Enforcing multifactor authentication (MFA) for privileged and remote users
- Controlling and monitoring access to critical systems
- Ensuring secure authentication even in offline environments

CMMC 2.0 Snapshot

3 levels based on risk – most manufacturers will need Level 2

Based on NIST 800-171 (110 security practices)

Final rule effective December 2024 → appearing in contracts in 2025

Unique access management challenges for manufacturers

Manufacturing environments introduce unique challenges to access management. Unlike a traditional corporate office, manufacturing facilities often have shared workstations on the plant floor, with limited or no connectivity, and a mix of modern and legacy systems. Operators, engineers, and technicians also frequently rotate shifts and use shared credentials, which increases risk and makes user accountability difficult.

Additionally, there's the critical need to balance security with uptime — a production line can't afford delays due to login issues or overly complex access workflows.

The reality is that access control must be secure and compliant, but it also needs to be fast, frictionless, and work with the systems and workflows already in place.

Chaitanya Yinti, VP of Product Management at Imprivata, explained, "If there's a cyber threat and you cut off your factory floor from the internet, you still must keep production going — without losing access control or audit logs. That's the kind of resilience manufacturers need."

Are your access points covered?

Common access points

Engineering workstations, shared human-machine interfaces (HMIs), remote portals (including those used by vendors or maintenance crews), industrial PCs, and systems such as supervisory control and data acquisition (SCADA), manufacturing execution systems (MES), enterprise resource planning (ERP), and product lifecycle management (PLM).

Often overlooked areas

Machine-level login points, like Windows-based or proprietary systems, and network-connected programmable logic controllers (PLCs). Without strong access controls and multifactor authentication, both can expose industrial environments to security risks.

Blind spots

USB ports and local admin access points can be exploited for lateral movement or data theft.

Checklist: Understanding the requirements of CMMC 2.0

Use the following list to align your security measures with CMMC 2.0. Each control helps reduce risk and improve audit readiness.

☑ Multifactor authentication (MFA) (IA.3.083)

Strengthening access security: requires users to verify their identity using two or more authentication factors before accessing systems containing controlled unclassified information (CUI)

Why it matters: prevents unauthorized access, phishing attacks, and credential theft

☑ Unique identification and authentication (IA.1.076)

Eliminating shared accounts: every user must have a unique identifier and authenticate before accessing systems

Why it matters: prevents the use of shared or generic accounts, ensuring accountability and traceability

☑ Password management (IA.2.078)

Enforcing strong password policies: requires strong, unique passwords and the implementation of password management policies

Why it matters: weak passwords remain a leading cause of breaches and unauthorized access

☑ Account lockout policy (IA.3.084)

Preventing brute-force attacks: locks a user's account after a certain number of failed login attempts

Why it matters: blocks attackers from using automated brute-force techniques to guess passwords

☑ Privileged account authentication (AC.2.056)

Securing admin and elevated access: applies additional authentication and controls to privileged accounts

Why it matters: only admin and privileged users should have access to critical systems to prevent attacks

☑ Authentication for remote access (AC.3.012)

Protecting remote connections: ensures that all remote access is secured with strong authentication measures, such as MFA

Why it matters: remote access is a major attack vector, making secure authentication essential

☑ Device authentication (IA.3.085)

Ensuring only trusted devices can connect: requires devices to authenticate before connecting to the network

Why it matters: prevents unauthorized or compromised devices from gaining access

☑ Session timeout and reauthentication (AC.2.010, AC.2.011)

Preventing unauthorized access from idle sessions: automatically locks a session or logs a user out after a period of inactivity

Why it matters: prevents unauthorized access if a user leaves a workstation unattended

☑ Cryptographic authentication (SC.3.177)

Encrypting credentials to prevent interception: uses cryptographic authentication to secure login credentials and prevent unauthorized access

Why it matters: ensures that passwords and authentication tokens are not intercepted or exposed

Now, let's look at best practices to include in your strategy to ensure compliance, security, and productivity in your access control and authentication approach.

Best practices to align compliance with productivity

In order for access control and authentication to support productivity — not slow it down — it needs to be built with your users, systems, and workflows in mind. Here are some best practices to consider:

Fits into the way your teams work.

Secure access should be fast and easy for frontline workers, helping them move through tasks without delay. On the IT side, your access program should reduce the time spent managing access issues like forgotten passwords or account lockouts.

Works with legacy and modern systems.

Most manufacturers are still working with legacy systems, and many frontline workers are accustomed to using the same tools they've relied on for years — like badges and shared workstations. Manufacturers need a way to move toward CMMC 2.0 compliance and stronger security without overhauling everything. That's why effective access control should support both legacy environments and newer technologies. Aligning with what's already in place helps drive adoption and avoid disruption — while still offering flexibility to scale with cloud-connected capabilities, modern authenticators, and open standards.

Supports offline access for uptime and business continuity.

Security threats sometimes mean taking an entire facility offline. When that happens, workers still need access to critical systems to keep production moving. With on-premises deployment options, workers can log in even if connectivity to the cloud or outside world is down, for any reason — ensuring operations continue without losing security controls.

Streamlines access for third-party contractors and remote workers.

Strong authentication ensures external partners get the access they need — no more, no less — without compromising security or requiring extra manual processes.

In the next sections, we'll share the key capabilities that support these best practices, followed by a framework for getting started.

> **"Access for the frontline workers and for the plant managers needs to be secure for sure, but it also needs to be frictionless, so that they can focus on the task at hand."**
>
> *— Sean Ryan, Senior Product Marketing Manager, Imprivata*

Key capabilities to consider for access control and authentication

So, what do you actually need to make access control and authentication work for both compliance and productivity? Every environment is different, but the capabilities below are commonly used across manufacturing and can help guide the right approach for your operations.

Single sign-on (SSO): Instead of juggling multiple passwords, workers log in once and get secure access to everything they need. While SSO is simple for modern apps, extending it to legacy systems can be challenging. That said, there are ways to make it easier, such as support for existing proximity badges and a wizard-based application profile generator that helps connect older applications without requiring new hardware.

Proximity badge authentication: Busy workers prefer to avoid long, complex passwords on a shared workstation. Badge tap authentication lets workers log in instantly while still enforcing security policies. If two-factor authentication (2FA) is required, they can enter a quick PIN after tapping their badge — making compliance fast and easy.

Biometric authentication (fingerprint and facial recognition): For workers in high-security areas, fingerprint or facial recognition provides additional low friction authenticator options to log in quickly without passwords, especially as a second factor when two-factor authentication is required.

Hard and soft tokens for two-factor authentication: When extra security is needed, workers can use a physical security key (e.g., YubiKey) or a mobile authentication app to provide strong protection without adding unnecessary steps.

Auditable access and user tracking: On a busy shop floor, dozens — or even hundreds — of workers may touch the same system or piece of equipment throughout the day. Tracking who did what is essential for compliance and security. Without proper authentication, many manufacturers resort to shared logins like "password12345," which makes it impossible to know who actually performed an action. With individual logins and badge authentication, manufacturers get a full audit trail without slowing anyone down.

Analytics, reporting and data capture: Reporting is not only about knowing who accessed what, when, and why. Robust analytics can help manufacturers spot access patterns, flag potential risks, and streamline compliance audits. "Data and analytics can help you spot things like unused equipment, unusual workstation use, and opportunities to improve efficiency or security," Yinti explained.

> “Many workers on the factory floor today just muddle through — typing passwords into systems never designed for them. It kills productivity. But there are better ways to both improve efficiency and provide better security. With the right strategy, you can get both.”
>
> *— Chaitanya Yinti, VP of Product Management, Imprivata*

Steps and tips for successful implementation

1. Start with discovery.

Begin by identifying who is accessing what, on which systems, and from where. This includes mapping users, roles, applications, and devices — especially those in OT environments that may not be managed by IT. Include discussions with end users to understand their behaviors, challenges, and workarounds.

2. Perform a risk assessment.

Once you understand your environment, assess where the greatest risks lie:

- What are your most sensitive systems (e.g., IP-heavy CAD tools, production planning systems)?
- Where are your biggest vulnerabilities (e.g., shared logins, lack of MFA)?

This will help you prioritize your efforts and tailor your strategy to what matters most based on risk, complexity, and business impact.

3. Define strategy and guide it with a phased approach.

Once your current state is mapped, the next step is to define access policies, user roles, and authentication methods. Consider: What levels of access are appropriate for each role? Will users need offline access? Should re-authentication be required after periods of inactivity?

There's a lot to account for when building a framework, which is why a phased approach is recommended — especially in manufacturing, where downtime and disruption are costly. Most organizations start with basics like eliminating shared passwords and deploying MFA for critical systems. Later phases might include integrating IAM with legacy OT systems, rolling out SSO, or implementing privileged access management (PAM) for admin users and 3rd party vendors.

Each phase should serve a clear purpose and move you closer to a stronger, more manageable access environment. **CMMC 2.0 isn't about perfection on day one — it's about steady progress that fits how your business operates.** "You're not expected to meet every aspect of CMMC right out of the gate. It's about proving you're moving forward, step by step," Ryan emphasized.

4. Select and implement the right technology.

With your roadmap in place, it's time to tackle the technology. This step will involve:

- **Solution selection:** choose IAM tools that support both IT and OT environments
- **Implementation:** integrate IAM across workstations, applications, directories, and networks
- **Testing and validation:** ensure security controls don't disrupt workflows or cause downtime

Again, consider the phased approach. You can run a smaller pilot first, validate the approach, and then scale it across the facility or facilities.

5. Establish governance policies.

Governance is critical for maintaining control, accountability, and ongoing compliance. Create clear, written policies that define how access is granted, managed, and revoked within your facility. For example, how will you onboard new users and assign role-based permissions? What happens when shifts change or someone leaves? How will you enforce strong password policies, including rotation and length or complexity requirements? These rules shouldn't just live in documentation — they need to be built into your systems and workflows, with automation wherever possible.

Finally, oversight is key — at the IT, security, and management levels — to regularly review access and provide sign-off when changes are needed.

> **"The plant managers are key partners in the success of a rollout. They're focused on ensuring uptime and making sure nothing disrupts the user or causes access issues on the floor."**
>
> *— Sean Ryan, Senior Product Marketing Manager, Imprivata*

6. Train users and manage change.

Change management can be the most challenging part of implementation. The key is to communicate early and often *why* the change is necessary (e.g., security, compliance, operational resilience) and *how* it will make work easier, not harder, for users.

Key tips include:

- Educate users, especially operators and engineers, on the new workflows and offer extra support during the rollout
- Collaborate with line workers and shift leads in pilot phases to identify friction and tailor solutions to real-world use cases
- Offer role-based training tailored to specific responsibilities
- Prioritize in-person, hands-on learning over generic online modules
- Roll out training in logical chunks, such as plant by plant or section by section
- Account for shift work by supplementing in-person training with short videos or on-demand refreshers and easy-to-follow documentation

The more personalized and interactive your training, the easier adoption will be.

7. Keep it going with audits and oversight.

Your access strategy shouldn't be a one-time effort. Regular audits help you spot gaps, track progress, and keep improving. Stay on top of governance by reviewing entitlements, monitoring usage, and updating policies as things change.

When it comes to CMMC 2.0 compliance, manufacturers can validate their progress by mapping their IAM implementation against NIST SP 800-171 — the framework that underpins CMMC Level 2.

Real-world success: A multinational manufacturer eliminates shared credentials and establishes a true "system of trust."

The challenge

A manufacturer wanted to remove all shared credentials to establish a "system of trust" that would resolve several challenges they were experiencing:

- Difficulty tracking individual user access across their systems, which prevented them from investigating the root cause of production issues
- Frequent process changes, which required workers to complete online training and submit certification — a difficult process for non-tech-savvy users
- Constant logging into LMS systems on shared tablets, which caused delays and frustration across IT and plant workers

The solution

Partnering with Imprivata, the manufacturer sought an access management solution that would reduce friction between operational leadership, IT, and front-line users while removing open systems access and security concerns. They found **Imprivata Enterprise Access Management (EAM) and Mobile Device Access**, which provided a consistent badge and PIN workflow to all shared endpoints (Windows and Android devices).

The result

The access management solution they implemented improved workflows for more than 19,000 users, especially in how they access MES systems and training. IT and plant teams alike saw fewer disruptions, faster access, and stronger accountability.

- Help desk calls for password resets and locked accounts dropped sharply
- Frontline user satisfaction with system access reached an all-time high
- Increased accountability and streamlined access are projected to save over 1 million hours annually

See access control in action on the manufacturing floor.

WATCH VIDEO ⟶

Are you ready for CMMC 2.0?

Manufacturers must work toward CMMC 2.0 compliance, but this effort can do more than meet requirements. With the right solution, it's also an opportunity to strengthen security *and* improve productivity at the same time.

With Imprivata, compliance doesn't come at the cost of productivity — it helps power it.

Imprivata offers a simple and secure access management solution built for the realities of manufacturing. The solution integrates seamlessly with legacy systems, minimizes disruption, and fits naturally into existing workflows — so frontline users stay productive.

The platform is flexible to deploy: You can run the solution on-premises with plant-level control, extend the solution with cloud-connected capabilities for advanced analytics, or choose a fully managed service that handles everything from onboarding to ongoing maintenance. The platform even keeps you covered when you need offline access control.

Explore Imprivata digital identity solutions for manufacturing

> **"When customers have the option to run access management service locally on-prem, in the cloud, or as a managed service, they don't have to spend their IT cycles deploying and maintaining it. And because Imprivata offers a total solution — from onboarding to maintenance and patching — they don't have to juggle multiple vendors either."**
>
> *— Chaitanya Yinti, VP of Product Management, Imprivata*

Imprivata is the digital identity company for life- and mission-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enable organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

Learn about the Imprivata difference

studio / ID BY INDUSTRY DIVE

studioID is Industry Dive's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

Learn more