imprivata

CASE STUDY

"It just worked." How Hamilton County Sheriff's Office achieved CJIS compliance with Imprivata

Challenge

- Urgent need to meet Criminal Justice Information Services (CJIS)-compliant multifactor authentication (MFA) requirements by October 1, 2024
- Workforce resistant to change
- Cybersecurity team of a cybersecurity director and one intern
- Poor password hygiene and high reuse across dozens of applications
- Even with a move to 20-character passwords as passphrases (per NIST guidance), 20% of employee passphrases were cracked during testing.
- Previous tools were either not secure, not user-friendly, or too expensive
- Difficulty finding a solution that was secure, sustainable, and easy to use

Organizational Profile

- **Organization Name:** Hamilton County Sheriff's Office
- **Location:** Hamilton County, Ohio
- **Type:** Law enforcement agency
- **Industry:** Public safety/ government
- **Size:** 900 users across 23 sites, managing more than 1,200 devices

Solution

- Implemented Imprivata Enterprise Access Management (EAM) for badge-based authentication
- Enabled passwordless authentication factors and password management through Imprivata
- Integrated system to allow one card for facility access, computer login, and MDC usage
- Tailored rollout, with the help of Imprivata's services team, to minimize disruption and ensure immediate value on day one

Results

- Reduced organizational password risk by an estimated 35-40%
- Significantly decreased helpdesk volume related to password resets
- Accelerated user adoption due to excitement about simplified login experience
- Deployed initial implementation in only three days using two staff members
- Full compliance achieved ahead of CJIS deadline with improved overall security

Challenge

When Jacqueline Ray took on the role of Director of Cybersecurity at the Hamilton County Sheriff’s Office, she had to build the agency’s first-ever cybersecurity program from scratch. The FBI’s Criminal Justice Information Services (CJIS) regulations required all agencies to have multifactor authentication (MFA) implemented by October 1, 2024, or risk being cut off from essential networks.

> **“We were cracking not just the old passwords but the passphrases, and they were still hackable.”**
>
> – Jacqueline Ray, Director of Cybersecurity, Hamilton County Sheriff’s Office

Ray was a team of one, with support from an intern. The department had 900 users, many of whom had been in their roles for decades and were resistant to change. Users were frustrated by complex password requirements and frequent resets.

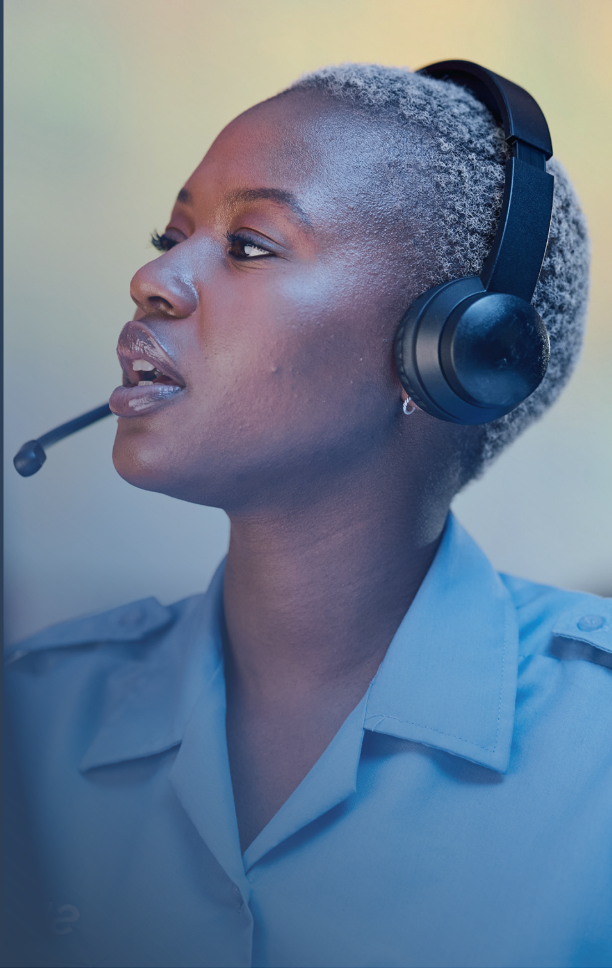
Efforts to implement longer passphrases did not yield better security. Even after increasing minimum password lengths to 20 characters, she found that 20% of passphrases were still vulnerable. “We were cracking not just the old passwords but the passphrases, and they were still hackable,” Ray said.

She needed a solution that was CJIS-compliant, sustainable for a small team, secure beyond checkbox compliance, and intuitive enough to win over a skeptical user base.

Solution

Ray explored multiple MFA options, including RSA keys and authenticator apps, but each presented roadblocks. Some were too costly, others too complex, and many posed privacy concerns for end users. None checked all the boxes. Then, a cold email from Imprivata caught her attention.

“I replied three minutes later because it mentioned CJIS compliance and badge-based login,” Ray recalled. The idea of using existing ID badges for authentication immediately resonated, especially given her background in the Department of Defense where CAC cards were standard. “It was a lightbulb moment,” she said.



Imprivata’s Enterprise Access Management solution allowed users to log in with a tap of their badge and a secure PIN. It worked seamlessly with encrypted prox cards that also functioned for facility access and MDC login. While employees no longer need to remember passwords, they are still in the system since backend systems and applications still rely on passwords. In order to make these more secure, the system also included a built-in password manager, allowing for secure application access without requiring users to remember or enter credentials.

Despite her small team, the initial rollout took only three days, including spinning up two servers and configuring the initial user profiles. “It was one of the easiest implementations of my IT career,” Ray said. “It just worked.”

Results

The impact of the implementation was immediate and significant. Password risk was cut by an estimated 35 to 40%. "Eventually, because the password is being passed in, they'll forget it. And that's the goal," said Ray. Plans are already in place to rotate passwords in the background, making credential theft from phishing attacks significantly harder.

> **I had users coming up to me saying, 'When is this coming? When am I getting mine?"**
>
> – Jacqueline Ray, Director of Cybersecurity, Hamilton County Sheriff's Office

Users who had been skeptical were now asking when they would receive their cards. "Literally, I had users coming up to me saying, 'When is this coming? When am I getting mine?'" she said. "They were thanking me, and they didn't even have it yet."

The streamlined system reduced help desk burden, eliminated the need for RSA token replacements, and made the IT environment more manageable. For a team with such a small cybersecurity staff, sustainability was critical.

Ray also highlighted the tool's ability to eliminate what she calls "Post-Deployment Attribution Bias" or P-DAB, a phenomenon where users blame new systems for unrelated issues. "If this tool wasn't easy to use or caused problems, I would've lost their trust," she explained. "Instead, I gained it."

imprivata®

Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. Imprivata's platform of innovative, interoperable access management and privileged access security solutions enable organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0) 208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533