Michigan.gov

A people-centered approach to modernizing statewide authentication

Award:	National Association of State Chief Information Officers (NASCIO) State IT Recognition Awards
Category:	Digital Experience: Enterprise Solutions
State:	Michigan
Project Start:	March 2025
Project End:	March 2026

Contact:

Kole Taylor
Information Technology Manager ITM-14
State of Michigan
Department of Technology, Management & Budget (DTMB)
TaylorK46@michigan.gov

EXECUTIVE SUMMARY

The State of Michigan modernized its authentication system by supplementing traditional password logins with Windows Hello for Business, a phishing-resistant biometric platform. This update gives users faster, more flexible authentication through facial recognition, fingerprint scanning, or a PIN. Affecting about 40,000 workstations statewide, the change strengthened cybersecurity, simplified access, and aligned with Zero Trust Architecture (ZTA) principles guiding future initiatives.

By introducing a structured enterprise organizational change management (EOCM) approach, the SOM achieved early voluntary adoption from nearly 10,000 employees before an enforcement date was announced. Importantly, there was no notable increase in authentication-related calls to the Customer Service Center (CSC) during or after the release of Hello, a success attributed largely to careful technical planning, strong interest, and participation through EOCM engagement activities.

By integrating modern identity technology with enterprise-wide change management, the SOM was able to build a resilient, future-ready authentication foundation that advances statewide security goals, improves employee experience, and positions SOM's enterprise to succeed at planned security initiatives in the future.

In addition to the technical and organizational successes of the rollout, the project's communication and support strategy proved central to its effectiveness. A comprehensive online resource hub became a highly visited source for self-service training, providing step-by-step job aids, a how-to video, and comprehensive FAQs. To date, the support site has generated over 18,000 views. This self-service model reduced anxiety, increased readiness, and reinforced confidence in the Hello rollout.

The communications cadence also played a major role in sustaining awareness. The first SOM-wide email introduced Hello and gave users an opportunity to enroll at their own pace. Then, messages were delivered over several months. Finally, three weeks before enforcement, then at two weeks, one week, the day before, and the day of rollout, giving employees clear guidance, and multiple avenues for support. This structured timing created predictability, reduced disruption, and drove high voluntary adoption across the enterprise.

IDEA

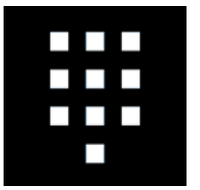
What problems or opportunities does the project address?

- With an ever-growing security-threat landscape posing increased risk to enterprises worldwide, enhancing security measures at all levels and embracing ZTA principles has become paramount in ensuring enterprise security. With both users and devices as common attack vectors, focusing on reducing password use and supplanting it with phish-resistant, device-bound credentials—in conjunction with policies preventing network access from non-managed devices—helps eliminate risky user behavior as well as the security risk from lost or stolen devices.
- For decades, logging into a workstation changed little, simple but inflexible; relying on a complex password used repeatedly throughout the day. Hello replaces this with facial or fingerprint recognition; phish-resistant methods that can securely pass authentication to enable single sign-on with Azure MFA. For a single individual, this saves time. Overall capacity efficiencies for the State Of Michigan are significant and help reduce password fatigue while increasing our security posture.
- The conclusion of this project dovetailed seamlessly with the implementation of the state's Secure Service Edge (SSE) project, which will require the reduction or elimination of RSA tokens used for authentication to VPN and other critical systems. The introduction of Azure MFA automatically through Hello effectively eliminates the need for RSA use in all but the most specialized situations.

- Through the EOCM processes, the SOM was able to focus on user engagement and facilitate enterprise change, which created additional collaborative communication opportunities focused on the "people" invested in this change. As a result, the cross-functional team was able to significantly raise awareness of additional services, such as the self-service password reset (SSPR). This created further enablement opportunities for users to recover from lost or expired passwords as well as reducing the need for CSC intervention.

Why does it matter?

- Updating authentication was critical for protecting SOM systems, safeguarding sensitive data, and preserving business continuity. Weak or stolen passwords represent one of the leading causes of breaches nationwide and continuing to allow legacy authentication methods places organizations at risk. By adopting Hello and Azure MFA, Michigan transitioned to phishing-resistant authentication that reduced reliance on reusable credentials, lowering the impact of lost credentials or even stolen devices.
- The operational benefits were equally important. Over the years, the demands associated with password resets and token management have significantly increased, imposing greater challenges on both users and support personnel. The implementation of Azure MFA and enhanced SSPR capabilities substantially mitigated these issues through streamlined processes and improved user awareness. This has allowed the CSC Help Desk resources to focus on troubleshooting complex issues, benefiting tens of thousands of SOM workers who rely on the CSC.
- Strengthening SOM's authentication practices also lays the groundwork for broader strategic improvements, supporting ZTA initiatives, improving alignment with National Institute of Standards and Technology standards, and preparing the organization for future passwordless capabilities.



Describe what makes the project innovative or distinct from similar initiatives.

- By applying structured EOCM practices, SOM shifted a technology rollout into a people-first initiative focused on employee readiness through communications, pilot testing, and strong executive alignment. This enterprise-wide effort engaged tens of thousands of devices and drove change both from the top—via consistent executive engagement—and from the bottom through open forums and word-of-mouth from early adopters.
- The project team conducted pilots, surveys, readiness assessments, communications campaigns, and training that drove unusually high voluntary adoption (nearly a quarter of the target population) and smooth enforcement across agencies with diverse and specific needs. The combination of technology expertise and change management made this a model project for any enterprise modernization, not simply security enhancements.

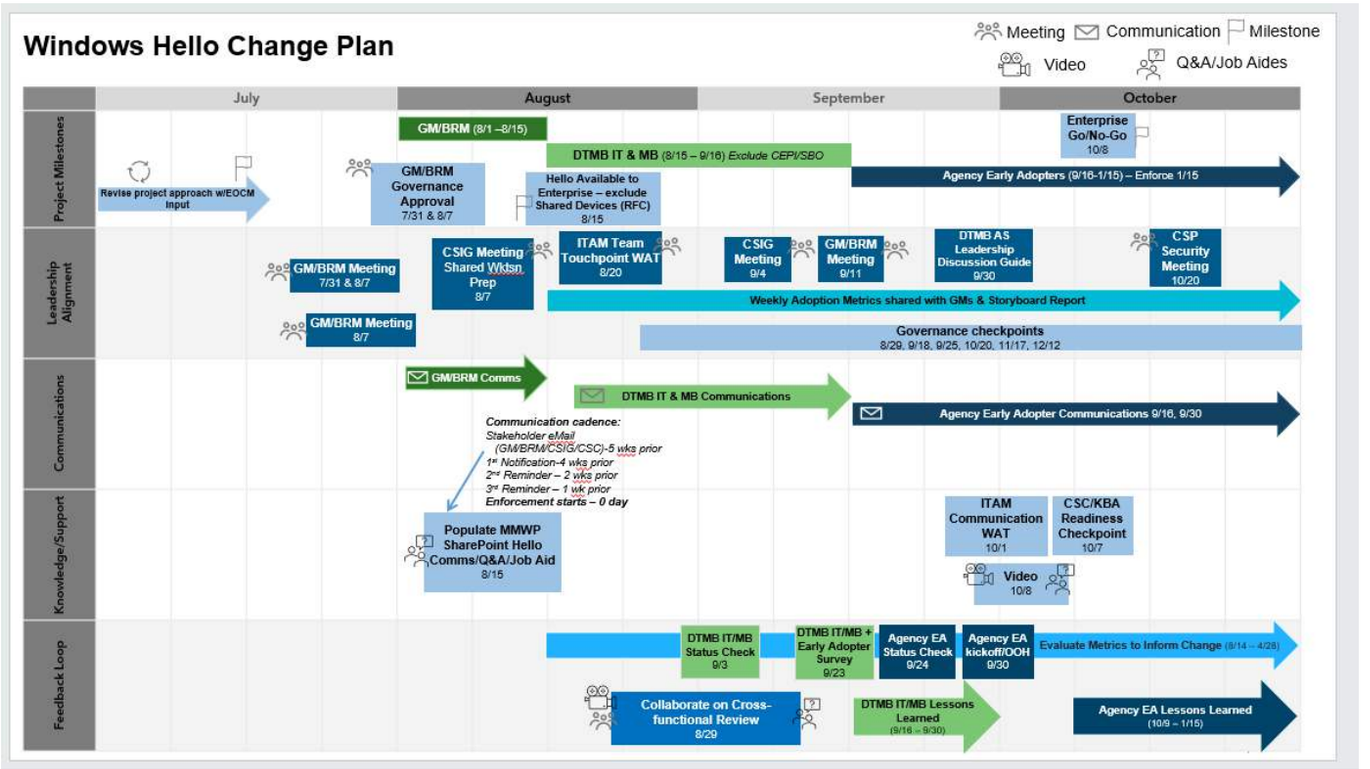
What makes it universal?

The security concerns addressed by this project are in no way unique to State of Michigan—nor even only to government entities. Modernizing security practices and improving posture is a critical need for all enterprises, public and private. As the threat landscape evolves, it is paramount that enterprise security landscapes evolve even more rapidly.

IMPLEMENTATION

What was the roadmap and how does this project fit into an enterprise view?

- The project followed an enterprise-wide waterfall methodology, structured to support consistent deployment across all agencies, minus users identified for early adopters. This approach ensured one coordinated rollout to conclude the project. The waterfall approach worked well with the EOCM pilot as the sequential structure allowed the team to build on processes as we were learning EOCM methodologies.



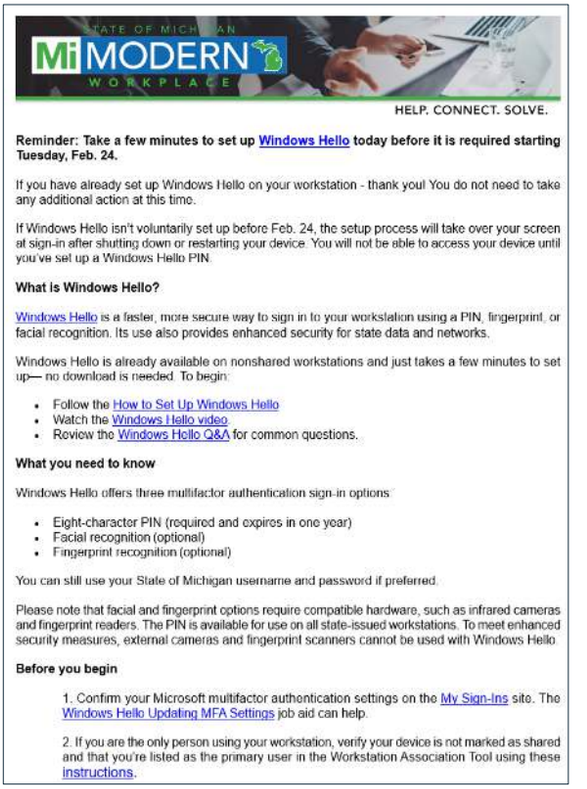
- The roadmap began with planning and testing, followed by a pilot phase to introduce and refine EOCM practices. Pilots validated communications, training, user readiness, and technical processes before scaling to the full enterprise. Once pilots showed readiness, the team executed a single enterprise-wide rollout supported by targeted communications and agency-specific engagement.
- Project success was measured using exit criteria written as S.M.A.R.T. objectives:
  - Enterprise-wide adoption at or exceeds 90% of applicable workstations
  - CSC support ticket counts have returned to pre-enforcement numbers
  - Field Services ticket counts have returned to pre-enforcement numbers
  - 14 days since last Incident Response or widespread issues resolution

Who was involved?

There were several key groups that were instrumental in the success of this project.

- **Executive leadership**. EOCM processes were being driven top-down by executive leadership, led by the director of Agency Services as well as State of Michigan's chief technology officer (CTO), with additional representation from leadership in the Project Management Office, Agency Services, Cybersecurity & Infrastructure Protection (CIP), and the Office of the CTO.
- **Project leadership**. A wide representation of unit-level management participated weekly or more in project meetings, informing progress and acting as key communication points for their respective teams.
- **DTMB Communications**. Tight integration with the DTMB Communications team ensured that they had direct, first-hand access to project information and personnel resources available to provide details necessary to support their mission in developing enterprise-wide communications.
- **Cybersecurity & Infrastructure Protection**. As a large-scale security initiative that lays the foundation for additional security project, CIP was involved from project instantiation through its conclusion, ensuring compliance with all NIST and other standards for compliance.

- **Client specialists**. A strong partnership with our population of employees who directly interface with, and support, agencies ensured that agency needs were identified, providing direct contact paths to facilitate problem resolution as needed. Client specialists were also instrumental in dissemination of information at ground level, reinforcing the enterprise-wide communications campaign.
- **EOCM vendor**. SOM contracted a vendor with expertise in EOCM to ensure methodological consistency with playbooks and other resources. The Windows Hello EOCM effort happened alongside additional EOCM projects, providing the opportunity to compare notes and learn from one another, driving awareness and interest in EOCM across the business. With Hello being the first and most mature project to complete, it helped provide valuable lessons to other projects.
  - The Hello project team had already begun planning when the opportunity to introduce EOCM arose, helping secure early buy-in. Strong executive support provided the resources needed to engage stakeholders and enabled enterprise-wide communications. These communications were timely, clear, and support-focused, consistently directing employees to online guides and FAQs


STATE OF MICHIGAN
MiMODERN WORKPLACE
HELP. CONNECT. SOLVE.

Reminder: Take a few minutes to set up Windows Hello today before it is required starting Tuesday, Feb. 24.

If you have already set up Windows Hello on your workstation - thank you! You do not need to take any additional action at this time.

If Windows Hello isn't voluntarily set up before Feb. 24, the setup process will take over your screen at sign-in after shutting down or restarting your device. You will not be able to access your device until you've set up a Windows Hello PIN.

What is Windows Hello?

Windows Hello is a faster, more secure way to sign in to your workstation using a PIN, fingerprint, or facial recognition. Its use also provides enhanced security for state data and networks.

Windows Hello is already available on nonshared workstations and just takes a few minutes to set up— no download is needed. To begin:

- Follow the How to Set Up Windows Hello
- Watch the Windows Hello video.
- Review the Windows Hello Q&A for common questions.

What you need to know

Windows Hello offers three multifactor authentication sign-in options:

- Eight-character PIN (required and expires in one year)
- Facial recognition (optional)
- Fingerprint recognition (optional)

You can still use your State of Michigan username and password if preferred.

Please note that facial and fingerprint options require compatible hardware, such as infrared cameras and fingerprint readers. The PIN is available for use on all state-issued workstations. To meet enhanced security measures, external cameras and fingerprint scanners cannot be used with Windows Hello.

Before you begin

1. Confirm your Microsoft multifactor authentication settings on the My Sign-Ins site. The Windows Hello Updating MFA Settings job aid can help.

2. If you are the only person using your workstation, verify your device is not marked as shared and that you're listed as the primary user in the Workstation Association Tool using these instructions.

How did you do it?

- The project implementation cost was approximately $285,000, all of which represented human resource hours dedicated to planning, technical implementation, communication development, eOCM activities, pilot coordination, and enterprise rollout. No major new software purchases were necessary, as SOM was already licensed enterprise-wide for Hello through its Microsoft agreement.
- The project relied on a multi-disciplinary team over a two-year timeline. Work began on April 9, 2024, with planning, early testing, and technical configuration, though the official start with EOCM included did not occur until March 2025. Active deployment and enforcement occurred through March 31, 2026, followed by the project's formal transition out of execution in late April 2026.
- From a technical standpoint, the rollout approach had little impact on the final outcome. The real value was in building enthusiasm and shaping a positive perception of the project. Regardless of methodology, the end state would have been the same: Windows Hello leveraging device TPMs and their built-in cryptographic keys to embed strong security on every primary SOM workstation. This device-level security also enables users to shift away from traditional passwords, supported by the growing range of Azure MFA-enabled services.

IMPACT

What did the project make better?

Technical Impact

- The Hello project delivered significant improvements across Michigan's cybersecurity posture, authentication experience, and operational efficiency. Before the project, authentication relied on cumbersome password entry and aging RSA tokens for VPN access which created security vulnerabilities, login issues due to human error, and increased demand for support. The new system replaced these methods with phishing-resistant biometric and PIN-based authentication, backed by device-bound cryptographic keys and Azure MFA. This shift aligned the state with ZTA standards, significantly reducing exposure to credential theft and phishing threats.

- Daily user experience improved in ways both subtle and distinct. Employees are no longer required to type complex passwords multiple times per day. Instead, they authenticate with fast, intuitive biometrics or a simple PIN, enabling smoother access to devices and remote systems. Survey feedback showed that 74% of users were either satisfied or very satisfied with Hello, with dissenting opinions largely focused on concerns about providing biometric data, which is not strictly necessary.
- By engaging EOCM processes early in the project lifecycle, SOM was able to pilot these new processes and apply the resulting insights effectively.
- Operationally, the project reduced friction and reclaimed IT capacity. Password-related help desk calls have slowed and are expected to continually reduce, aided by the adoption of self-service password reset (SSPR) capabilities. The retirement of RSA tokens is ongoing but will reduce administrative costs. Through these various efficiencies, SOM has been able to provide better security and user experience while reducing overhead of support.
- Finally, and importantly, this project was a foundational element in paving the way for additional ZTA initiatives, such as SSE and passwordless authentication.

EOCM Impact

- Engaging EOCM processes early in the project lifecycle allowed the team to pilot new methodologies and approach the work from a broader, more strategic perspective. By introducing change management practices even before the pilot phases, SOM gained the ability to evaluate the project through a different lens, providing insight into both the technical and human factors to increase enthusiasm for adoption. These early insights proved invaluable and have since informed other initiatives, including major efforts like SSE, demonstrating that the lessons learned in this project have immediate and long term value across DTMB.
- EOCM also helped us identify and analyze stakeholders early, before communications began. Instead of treating the effort as purely technical, SOM used EOCM tools to map affected groups, gauge impact levels, and anticipate where additional support was needed to prevent resistance. The impact radius assessment clarified who would be affected and how significantly, guiding where to focus resources and action.
- This assessment directly informed our communication and engagement strategy. By ranking audiences by impact and readiness, we could prioritize messaging, tailor content, and sequence outreach to match user needs. High-impact groups received earlier, more detailed communication, while lower-impact audiences were engaged closer to deployment. This intentional approach kept statewide messaging clear, timely, and appropriately scaled. In short, EOCM wasn't an add-on—it was a foundational element that strengthened execution, improved user experience, and set a repeatable model for future enterprise initiatives.

How do you know?

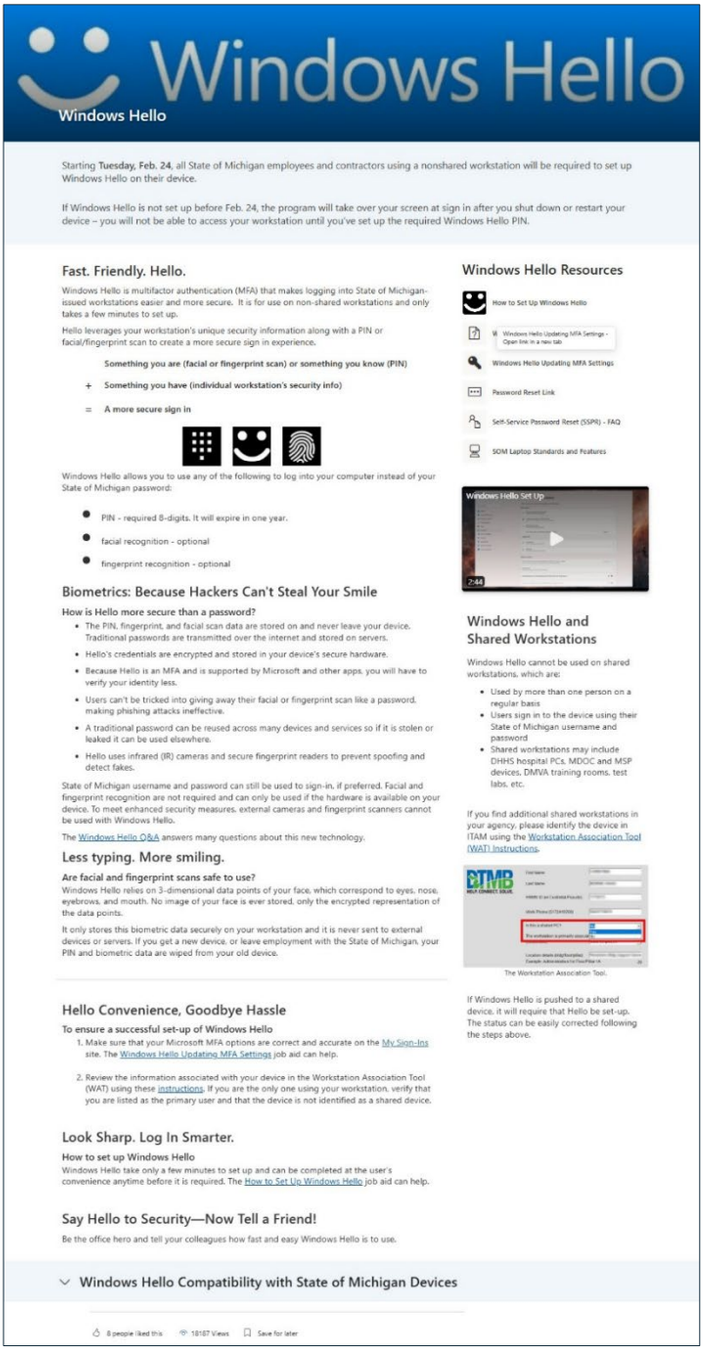
- Early rollout data showed widespread user approval, with pilot feedback indicating high satisfaction and ease of setup, and usage reaching 85,000+ Windows Hello sign-ins per week, even before the final enforcement date. One month after project completion, that number rose to over 200,000 Hello sign-ins per week. Nearly 39,000 users are now configured to use Hello. These results confirm that the new

authentication model not only strengthened security but also made routine access simpler and faster for SOM employees.

- The effort focused on improving the daily authentication experience and strengthening Michigan's workstation security as a foundation for Zero Trust and future passwordless capabilities. These outcomes, while not monetary, represent critical investments in security maturity and user experience, and help mitigate hard-to-quantify risks such as lost or stolen passwords, compliance gaps, and enterprise-wide vulnerabilities.

What now?

- Windows Hello is expected to drive sustained operational efficiencies by reducing password-related inquiries to the CSC. With intuitive biometric and PIN-based login methods, employees experience fewer lockouts and require fewer password resets, decreasing first-level support calls. As calls decrease, CSC technicians can focus on higher-complexity issues, improving service quality, and reducing wait times across the enterprise.
- The online support hub created for the Windows Hello rollout will remain in place, ensuring long-term value beyond the initial implementation. With over 18,000 views, it proved to be a highly relied-upon resource during the transition. Its job aids, how-to video, and curated FAQ help employees complete setup independently and answer common questions without contacting the CSC. Keeping this resource available ensures that employees continue to benefit from accessible, high-quality guidance whenever they need it.
- Keeping the site active is especially important for new employees to adopt Windows Hello as their standard authentication method. Rather than recreating training or issuing repetitive communications, agencies can direct incoming staff to a trusted resource already validated by thousands of users. The page serves as an always-available guide for onboarding.



The Windows Hello for Business rollout demonstrates how the State of Michigan can successfully pair modern security upgrades with thoughtful, enterprise change management to deliver meaningful, sustained improvements. By combining strong technical execution, clear communications, and a people-centered approach, the project not only strengthened authentication statewide but also created a repeatable model for future modernization efforts.