

San Marcos USD

Securing Education with
Passwordless Multi-Factor
Authentication





SAN MARCOS
UNIFIED SCHOOL DISTRICT

ENGAGING STUDENTS... INSPIRING FUTURES

INDUSTRY

Education

END USER

San Marcos Unified School District (SMUSD)

DEALER

Identify Systems

PROJECT TYPE

Multi-Factor Authentication (MFA)
Implementation

SCOPE

Deployment of Hirsch's uTrust FIDO2 Security Keys for 2,500 employees across multiple school sites to enhance cybersecurity and meet insurance requirements.

HIRSCH SOLUTIONS

uTrust FIDO2 Security Key

“ Hirsch's uTrust FIDO2 Security

Keys have been pivotal in
enhancing our cybersecurity
while supporting our mission to
use technology responsibly.

They're secure, user-friendly, and

budget-friendly. ”

Tony Cabral

Coordinator of Technology
Operations, SMUSD





The Challenge

San Marcos USD needed robust cybersecurity to combat rising threats and comply with stringent insurance mandates, without relying on personal devices for authentication.



The Solution

SMUSD partnered with Hirsch and Identify Systems to deploy uTrust FIDO2 Security Keys, providing secure, user-friendly MFA across its workforce.



The Next Steps

SMUSD plans to monitor key performance and explore further cybersecurity enhancements with Hirsch's solutions.

Business Situation

San Marcos Unified School District, a leading K-12 institution in California, serves thousands of students and 2,500 staff across multiple campuses. Facing escalating cyber threats—ransomware, phishing, and data breaches—the district needed to strengthen its security posture to protect sensitive student and staff data. Updated insurance requirements mandated multi-factor authentication (MFA), but staff reluctance to use personal devices for authentication posed a challenge. SMUSD sought a cost-effective, compliant, and user-friendly solution to secure its digital infrastructure while aligning with tight educational budgets.

Technical Situation

SMUSD's existing authentication relied on passwords, leaving systems vulnerable to cyber threats. The district considered mobile-based MFA but faced pushback from employees unwilling to use personal devices. Key challenges included:

- **Cybersecurity Risks:** Rising phishing and ransomware attacks threatened data security.
- **Compliance Needs:** Insurance mandates required NIST-compliant MFA.

- **User Adoption:** Solutions needed to be intuitive to ensure staff compliance.
- **Budget Constraints:** High-cost or licensed solutions were unsustainable.

Identify Systems recommended Hirsch's uTrust FIDO2 Security Keys for a hardware-based, cost-effective MFA solution.

Solution

Hirsch delivered a tailored MFA solution, deploying uTrust FIDO2 Security Keys across SMUSD's 2,500 employees. Key features included:

- **uTrust FIDO2 Security Keys:** Provided phishing-resistant, authentication without personal device reliance.
- **Flexible Enrollment:** Offered three options via ClassLink SSO, SMS, or keys, with clear instructions and a help desk for support.
- **Seamless Deployment:** Keys were distributed to all school sites, with a mandatory enrollment deadline ensuring adoption.

Hirsch's support team and Identify Systems ensured smooth implementation, minimizing disruption and maximizing security.

