CASE STUDY

Product: **NIM** Sector: **Education** Date: **2026**

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

EACS
EAST ALLEN COUNTY SCHOOLS
DREAM IT. DO IT.

Replacing Legacy Account Management with Centralized User Lifecycle Management

Managing identities across multiple systems had become increasingly complex for East Allen County Schools. Legacy automation tools, disconnected directories, and manual auditing processes created operational friction and security risk. To modernize its identity management approach and regain control over user lifecycle processes, the district implemented NexGen Identity Management (NIM), enabling a more flexible, transparent, and secure foundation for account provisioning and governance.

Challenges Before NIM

Before adopting NIM, the district relied on outdated and legacy automation systems to manage user accounts. Troubleshooting inconsistencies across multiple directory systems was time-consuming, particularly when user records were incorrect or when HR data did not align across systems. The rigidity of the legacy environment also prevented the district from updating its account creation processes to meet evolving cybersecurity requirements.

Auditing posed another significant challenge. Reviewing accounts required manual CSV exports, repeated data comparisons, and LDAP tools to bulk-deactivate or delete users. These processes were inefficient, error-prone, and difficult to scale as the organization grew.

Evaluation and Selection of NIM

Mitchell Locke, the System Engineer at East Allen County Schools, evaluated several identity management solutions before selecting NIM. While other options were considered, NIM stood out for its ability to integrate directly with the district's Student Information System (SIS) via API connections. These integrations significantly reduced reliance on manual exports and imports, streamlining data flows and reducing administrative overhead.

Key Product Highlights

NIM provided East Allen with a modern identity management platform that fully replaced its legacy systems. With built-in onboarding tools and clear documentation, the IT team can independently troubleshoot provisioning issues and create new workflows without third-party assistance. They now ensure that all user accounts comply with current Acceptable Use Policy (AUP) requirements and can quickly establish role-based security groups in Google and Active Directory. Additionally,

Client

East Allen County Schools

Challenge

Legacy identity systems created inconsistencies across directories, required manual audits, and limited the district's ability to adapt to evolving security and user management needs.

Solution

East Allen implemented NIM to centralize identity data, automate provisioning and deprovisioning, integrate with HR and SIS systems, and enable in-house workflow management.

Products and Connectors

- RDS
- Google
- Active Directory
- Skyward QMlativ through the OneRoster API

Result

The district improved security, streamlined account management, eliminated reliance on third-party support, and ensured users have accurate, role-based access with minimal administrative effort.

CASE STUDY

Product: **NIM** Sector: **Education** Date: **2026**

> *“NIM has been an excellent purchase and addition to our suite of identity management products. It will help you grasp the identity sprawl you have, clean it up, and assist you in maturing your identity management process. It also just works. It is not a product we have to constantly be watching. It can handle any K12 workload.“*

Mitchell Locke
System Engineer

NIM enables easy auditing across HR, SIS, Google, and Active Directory systems, strengthening security and ensuring users have only the access necessary to perform their roles.

A particularly valuable capability of NIM is its tabular view of directory data. Although not a primary focus during implementation, this feature quickly proved essential for handling internal data requests, enabling staff to extract accurate information efficiently. By consolidating data from Active Directory, Google, HR, and SIS systems, NIM delivers a centralized, reliable source of truth for identity information across the district.

Integration and Adaptability: NIM integrates seamlessly with the district’s existing infrastructure. The district connects to Skyward Qmlativ via the OneRoster API, as well as to Active Directory and Google using API-based connectors. For systems without API capabilities, such as the district’s HR system (RDS), NIM easily ingests CSV exports without disruption.

Additionally, the Google Sheets connector enables one-off account management scenarios, such as validating AUP signatures and maintaining accurate contact information. Across all integrations, NIM has proven reliable and stable.

Enhanced Efficiency and Productivity: With NIM in place, identity management has largely become a background process. Automated provisioning and deprovisioning allow the IT team to focus on higher-value initiatives rather than routine account maintenance. When issues do arise, they can be quickly identified and resolved internally without external assistance.

The district also eliminated the need to manually track employee departures through board reports, as account changes are now driven directly by authoritative HR data.

Security Enhancement and Compliance: NIM significantly improved accountability and visibility across user access. Detailed logging makes it clear who performed specific actions and when. Automation ensures that users receive only the access they need, with permissions automatically adjusted as roles change.

When exceptions are required, NIM supports controlled overrides that are fully tracked and documented, ensuring transparency without compromising security. These capabilities have strengthened the district’s overall security posture while maintaining operational flexibility.

Consultancy and Support

The implementation process was smooth and collaborative. A dedicated software consultant assisted with installation, system setup, and initial configuration. After a short testing period, NIM was fully operational and aligned with the district’s requirements.

Following onboarding, the district transitioned to general customer support. Support interactions have been infrequent, but consistently positive. Questions are typically resolved with a single, knowledgeable response.

Future Outlook and Endorsement

Looking ahead, the district plans to further mature its identity program by implementing a full role-based access control (RBAC) system. NIM is already supporting this initiative during the design phase and continues to adapt to evolving requirements. This aligns with the district’s broader adoption of CIS cybersecurity controls.

The district strongly endorses NIM for similar organizations, citing its stability, adaptability, and ability to handle the demands of large K–12 environments with minimal ongoing oversight.

Conclusion

NIM has proven to be a reliable, flexible, and scalable identity management solution for this K–12 district. By eliminating legacy systems, reducing manual effort, improving security controls, and enabling in-house management, NIM has helped the organization regain control and advance its cybersecurity maturity.