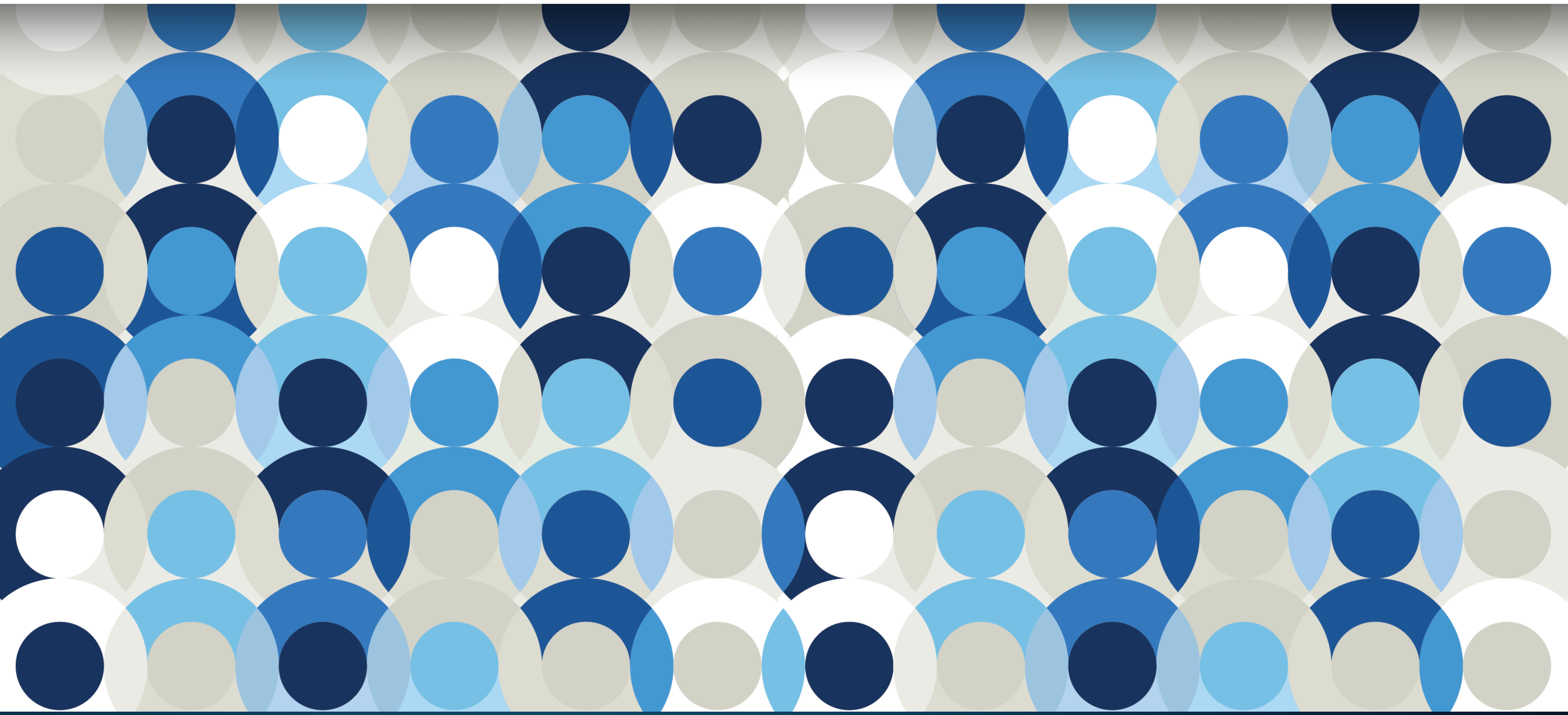
Author(s): Unicon, Inc.
Date: June 2025



IAM in Higher Ed: Different by design, misunderstood by commercial vendors

Understanding the technical, business, organizational, and lifecycle differences that set higher education apart from corporate IAM solutions like Okta, Sailpoint, and Microsoft Entra

Author(s): Unicon, Inc.
Date: June 2025

IAM in Higher Ed: Different by design, misunderstood by commercial vendors

Understanding the technical, business, organizational, and lifecycle differences that set higher education apart from corporate IAM solutions like Okta, Sailpoint, and Microsoft Entra

Executive summary

When evaluating Identity and Access Management (IAM) solutions, it seems reasonable for institutions to adopt commercial platforms that appear feature-rich, competitively priced, and widely used across the corporate sector. However, the operational and governance realities of higher education differ in fundamental ways from those of the private sector. These differences have significant implications for IAM design, implementation, and long-term sustainability.

Higher education institutions manage identities for diverse and dynamic populations: students who also serve as employees or teaching assistants, alumni who reengage as graduate students, faculty with cross-institutional research affiliations, and a range of short-term and sponsored users. The academic calendar drives cyclical changes in role assignments, and authority over identity and access decisions is often distributed across schools, departments, and administrative units.

Commercial IAM tools are built for centralized enterprise environments and often struggle to accommodate the structural and operational complexity found in higher education. Their underlying assumptions about organizational hierarchy, lifecycle simplicity, and top-down governance may result in rigid architectures, costly customization, and insufficient support for federated access and delegated administration. For higher education institutions, implementing popular commercial IAM solutions like Okta, SailPoint, and Microsoft Entra (Azure AD) can introduce higher costs and increased complexity in configuration and long-term management, particularly when adapting to academic calendars and decentralized control.

This paper explores:

- The structural and functional differences that distinguish IAM in higher education
- The hidden costs and limitations of retrofitting commercial IAM solutions for academic environments
- A higher education-native alternative in Unicon’s Navigate IAM, built on open standards and tailored for institutional realities

With insights from Unicon’s experience implementing both commercial and open IAM systems, we argue that **universities are best served by solutions designed specifically for the governance models, lifecycle dynamics, and collaborative needs of higher education.**

IAM in Higher Education is structurally different by design

At first glance, many of the functional requirements for Identity and Access Management (IAM) in higher education may appear similar to those in corporate environments: institutions must provision and de-provision users, enforce authentication policies, enable single sign-on (SSO), and ensure secure access to systems. But beneath these surface similarities lies a fundamental architectural mismatch. Higher education's identity lifecycles, user types, and governance models introduce challenges that corporate IAM tools were never designed to address.

IAM Characteristic	Higher Education	Corporate IAM
Role Structure	Overlapping, fluid, and temporary roles (e.g., student + employee + alumni)	Stable, mutually exclusive job roles
Identity lifecycle	Term-based; roles change frequently with academic calendar and affiliation types	Event-driven (hire, promotion, termination)
User populations	Millions of users, including alumni, applicants, guests	Tens of thousands of internal users
Federation needs	Essential for research collaboration (e.g., InCommon, eduGAIN) and facilitating shared educational resources (e.g. course sharing)	Optional or rarely needed
Governance model	Decentralized; authority distributed across departments and colleges	Centralized under IT or security leadership
Scalability requirements	Must support large, long-lived identity datasets	Optimized for known user base size
Typical calendar cadence	Semester- or quarter-based identity changes	Optimized for known user base size
Identifiers	Multiple, concurrent identifiers required (e.g. ERP, IAM, NetID, Library, Photo ID)	Typically, very few concurrent identifiers

Complex and overlapping roles

Higher education institutions support a wide range of user roles, commonly including situations in which a single individual holds multiple identities simultaneously. A student may also be a research assistant, resident advisor, or university employee — all at the same time. Faculty may serve as department chairs, principal investigators, or cross-registered instructors at partner institutions. Alumni may return as graduate students or be reactivated as adjunct faculty years after graduation.

Traditional role-based access control (RBAC) models, common in corporate IAM systems, assume static or mutually exclusive roles. In higher education, roles are fluid, intersecting, and often temporary. This demands more granular, context-aware access policies, and IAM systems that can represent and enforce them without fragile workarounds.

Commercial IAM platforms typically provide a limited schema hierarchy designed to support straightforward corporate directory models, consisting of:

- Primary user profile
- Job title
- Department, and
- Entitlements tied to group membership

These systems are optimized for environments where a user has one role at a time, and where access decisions follow linear reporting structures. Even faculty reporting relationships can be complex, where a faculty member may be a department chair while also serving appointments at different levels in multiple departments or colleges, such as promotion and tenure committees.

Attempting to model the complexities of university roles within the out-of-the-box schema of a commercial IAM system requires overloading attribute fields, creating dozens of custom profile fields, or maintaining external systems to manage role logic. This increases implementation complexity and introduces long-term maintainability issues. Institutions find themselves building fragile workarounds just to reflect relationships that are native to academic environments. These are relationships that higher education-native IAM tools like midPoint and Grouper are purpose-built to model and enforce.

Lifecycle management on an academic calendar

Unlike corporations, where onboarding and offboarding are relatively stable and event-driven, higher education operates on a term-based calendar that creates predictable but frequent shifts in user status. Students enroll, drop courses, or change majors mid-term. Teaching assistants are assigned on a per-course basis. Staff and faculty often operate on academic-year contracts, sabbaticals, or seasonal employment models, often requiring access to resources before their employment date begins.

This dynamic environment effectively creates “merger-and-acquisition-level” identity changes several times a year (at the start of each term) requiring IAM systems that can handle rapid, large-scale transitions with minimal manual intervention.

Lifecycle management within higher education IAM environments presents significant technical complexity due to the simultaneous and cyclical nature of user-status transitions. Unlike corporate systems, where changes in employee status (onboarding, promotions, terminations) typically occur sporadically and can be easily triggered by event-driven workflow, academic institutions face predictable yet high-volume, term-based changes that happen concurrently. This requires IAM systems to execute batch processes at a massive scale, efficiently onboarding thousands of users at term start, and rapidly adjusting roles or removing access at term end. Additionally, mid-term changes, such as students assuming new roles like teaching assistants, demand intricate conditional logic and overlapping role management capabilities. Traditional IAM systems, often designed around linear HR processes, struggle to handle this complexity without extensive customization, external scripting, and dedicated maintenance, increasing both technical burden and risk.

Federated identity and research collaboration

Higher education is inherently collaborative, and this collaboration increasingly depends on federated identity systems. Researchers, instructors, and students routinely require access to systems and datasets hosted at other institutions or with partner organizations. From scientific computing environments and grant-funded data repositories to shared teaching platforms, institutions must support cross-organizational authentication without compromising security or administrative control.

To meet these demands, most institutions rely on federated identity standards such as SAML, implemented through frameworks like InCommon and eduGAIN. These frameworks allow users to log in with their home institution credentials while accessing third-party services. Doing so preserves privacy, reduces account sprawl, and enhances usability. However, many commercial IAM platforms treat federation as a non-core feature. Then they find themselves requiring complex configuration, third-party extensions, or additional licensing to achieve even baseline interoperability.

This is not a peripheral use case. In addition to research collaboration, federated identity is becoming essential for course-sharing initiatives, allowing students to enroll in and access courses hosted at partner institutions through consortia or system-wide agreements. These arrangements, which rely on standards-based federated login, are seeing renewed interest as institutions explore shared service delivery models and expanded access opportunities . As this trend accelerates, **IAM systems must treat federation not as a feature to be bolted on, but as a core architectural requirement.**

Commercial solutions often fall short here. Their federation support may be limited to basic SAML integration, with no native awareness of academic federation frameworks or the nuanced identity assurance profiles used in research and teaching collaborations. In contrast, platforms like Shibboleth are designed from inception to support federated trust, metadata management, and identity attribute release policies that align with academic norms.

Institutions engaged in research and multi-campus teaching efforts need IAM infrastructure that is not only standards-compliant but also fundamentally aligned with the architectural and policy requirements of academic federations. Commercial IAM platforms like Okta and Entra are not built to support this model. Their integration patterns typically assume one-to-one relationships between identity providers (IdPs) and service providers (SPs), requiring manual setup, individual metadata exchange, and per-SP attribute release policies.

This is fundamentally incompatible with the federation model used in InCommon and eduGAIN, where one IdP must be discoverable and trusted by thousands of SPs through a shared metadata framework.

Effective federation requires capabilities such as consuming aggregate or MDQ metadata, interpreting entity category tags for automated attribute release (e.g., Research & Scholarship), registering IdPs using institutionally owned domains, and optionally prompting users for attribute consent to meet privacy and compliance obligations. These are foundational to scalable, trust-based collaboration across institutions. Without them, IAM systems introduce friction, limit access, and create operational bottlenecks that are unsustainable in the context of higher education and research.

The incompatibility of commercial IAM with scalable federation for Higher Ed and research

At a technical level, the architectural assumptions of commercial platforms like Okta and Entra are incompatible with scalable federation as required in higher education and research. These platforms enforce a one-to-one integration model: each service provider (SP) requires manual configuration, a distinct IdP entity ID, and a tailored attribute release policy. This does not scale in a world where institutions may need to connect to thousands of SPs, many of which the central IT team may not even know about in advance.

In contrast, federated IAM frameworks like InCommon and eduGAIN support a one-to-many trust model. A single IdP can interoperate with thousands of SPs using shared, community-curated metadata and standardized attribute release categories.

Commercial IAM tools typically fail to support the following foundational federation capabilities:

1. **Federation metadata consumption**. They cannot consume aggregate metadata files or query metadata on demand using MDQ (Metadata Query) protocols.

2. **Standards-compliant IdP registration.** Their IdPs often use entityIDs rooted in vendor-owned domains (e.g., okta.com, windows.net), violating federation policy requirements that entityIDs must be rooted in a domain under institutional control.

3. **Federation-specific metadata interpretation.** They lack support for federation markup such as entity categories and policies required to automate attribute release (e.g., Research & Scholarship entity category, which enables trusted service providers to receive attributes automatically without requiring custom rules for each one).

4. **Policy-based attribute release.** They are not capable of releasing attributes based on federation tags rather than per-SP configurations.

5. **Decentralized metadata change management.** Without federation infrastructure, all SP metadata changes must be handled manually, increasing administrative burden and risk.

6. **User consent handling.** Most commercial IAM tools lack support for customizable user consent prompts tied to attribute release, which is a critical requirement for FERPA compliance and institutional data governance.

These gaps are not merely incidental; they reflect deep architectural differences. Federation in higher education is a scalability strategy, a compliance requirement, and a cultural necessity. The inability of commercial IAM systems to foundationally support this model explains why institutions reliant on research partnerships, cross-institutional teaching, or shared services often encounter significant barriers to full adoption.

One-to-one vs. One-to-many: Why federation doesn't fit the corporate model

Model	Corporate IAM (e.g. Okta, Entra)	Federated IAM (e.g. Shibboleth + InCommon)
IdP-SP relationship	One-to-one, manually configured	One-to-many, automatically trusted via metadata
Metadata	Local, manually entered per SP	Shared, centrally maintained, MDQ/ aggregate
Attribute release	Per-SP configuration	Policy-driven via federation categories
Consent support	Typically absent	Supported and configurable per SP/policy
Entity ID	Rooted in vendor domain	Required to be in institutional domain
Scalability	Manual integration for each SP	Auto-discovery and trust for thousands of SPs

Millions of users, one identity platform

A typical large university manages millions of identity records across students, alumni, faculty, staff, prospective applicants, and guest users. Most commercial IAM platforms are optimized for enterprises with tens of thousands of users and not multi-faceted universities with millions of accounts. As a result, institutions face performance degradation, pricing penalties, or forced trade-offs about who is included in the identity system.

In contrast, higher education must maintain lifelong identity relationships, particularly with alumni, who may re-engage through giving, mentorship, or continuing education programs. IAM platforms must therefore support long-term scalability without introducing cost barriers tied to user volume.

Flexible governance opportunities

Finally, the organizational structure of higher education introduces a level of decentralization rarely seen in the private sector. Colleges, departments, registrars, IT groups, and research centers often operate autonomously, each with their own policies, systems, and access needs. Top-down mandates, such as institution-wide multifactor authentication (MFA) or access attestation, are rarely effective without stakeholder buy-in and delegated authority.

IAM systems must reflect this decentralized reality, enabling fine-grained delegation of administrative control, policy enforcement, and approval workflows. Corporate IAM tools, designed for centralized IT ownership under a single CIO or CISO, often lack the flexibility to support this model.

Where commercial IAM solutions fall short

Despite their prominence in the marketplace, commercial IAM platforms like Okta, SailPoint, and Microsoft Entra (Azure AD) are fundamentally designed for corporate environments where there's often centralization, uniformity, and linearity. When applied to higher education, these tools often require significant customization, third-party extensions, and architectural compromises. This mismatch is not merely a matter of feature gaps; it stems from a structural misalignment between corporate IAM assumptions and the operational realities of academic institutions.

Built for corporations, not campuses

Commercial IAM solutions are optimized for organizations with centralized IT departments and clearly delineated roles. Their data models, user provisioning flows, and policy enforcement mechanisms assume static job titles and hierarchical reporting structures. In higher education, where governance is distributed and individuals often assume multiple concurrent roles, these assumptions break down quickly.

As a result, institutions are often forced to bend academic role structures to fit corporate schemas. This introduces brittle customizations, delaying implementation timelines, and increasing long-term maintenance burdens.

Limited support for role complexity and attribute-based access

Most commercial platforms claim to support overlapping roles or dynamic access control, but in practice, their implementations are often shallow. For example, many tools rely on static role assignments or basic entitlements that cannot account for the nuanced, attribute-driven access needs of academic environments.

This becomes a critical issue in decentralized institutions with multiple campuses or colleges. Determining which users are teaching assistants for a specific department, or managing access policies that reflect enrollment status, course load, or academic standing, requires systems that support policy- and attribute-based access control at scale. This capability is often absent or underdeveloped in commercial solutions.

Federation treated as an afterthought

For higher education institutions engaged in collaborative research or inter-institutional partnerships, identity federation is not optional, but foundational. Standards such as SAML and initiatives like InCommon and eduGAIN are essential for enabling secure, seamless access across organizational boundaries.

Yet many commercial IAM products treat federation as an advanced feature or bolt-on integration. Institutions often must rely on middleware, third-party tools, or vendor-specific federation gateways, which introduce additional points of failure and complexity.

No model for delegated administration

Corporate IAM tools are built around centralized IT governance, assuming a small number of administrators with global authority. In contrast, higher education institutions require fine-grained delegation of access control and identity management functions to reflect the institution's governance culture.

Faculty may control access to research systems. Registrars may manage course-level entitlements. College deans may need oversight without direct administrative responsibility. Without support for delegated administration, institutions are forced to route all IAM-related changes through a central team, creating bottlenecks and eroding local autonomy.

Closed architectures and limited extensibility

Most commercial IAM vendors offer black-box software with limited opportunities for customization or introspection. Institutions that need to adapt the system to support specific workflows, integrate with legacy systems, or meet evolving compliance requirements may find themselves constrained by vendor roadmaps and opaque APIs.

Furthermore, closed ecosystems often discourage innovation and increase vendor lock-in. Extensions, connectors, or analytics tools may be available only through proprietary licenses or partners, limiting flexibility and increasing total cost of ownership over time.

The hidden costs of misaligned IAM efforts

Many higher education institutions have implemented commercial IAM solutions and continue to use them as part of their broader identity strategy. However, even in successful implementations, institutions often encounter trade-offs, limitations, or unexpected complexities that affect long-term outcomes.

One common observation from IAM evaluations is that commercial platforms tend to handle a narrow band of enterprise use cases well. These typically include provisioning and access control for core systems such as HR, SIS, or LMS. But when it comes to modeling multiple concurrent roles and affiliations, commercial platforms often require additional manual oversight. The systems may struggle to maintain consistent identity states for users who hold simultaneous jobs, such as a staff member who is also teaching, or who move between roles mid-term (a frequent occurrence in higher education).

Another limitation is in delegated administration. Commercial solutions often assume centralized IT ownership of access control, which makes it difficult for departments, research units, or functional areas to manage roles and entitlements directly. As a result, institutions end up managing access to many systems within the services themselves rather than through the IAM system. Gaps often occur in deprovisioning when a user's institutional role changes but downstream access is not revoked. It also undermines efforts to build a comprehensive, centralized view of who has access to what and why, which is a foundational principle of Zero Trust Architecture.

Institutions report unexpected costs and constraints after selecting a commercial IAM product. Features such as delegated role management or federation may be licensed separately or require third-party support, even when they were assumed to be included during procurement. Such surprises can extend implementation timelines and strain internal resources.

Vendor continuity is another emerging concern. When commercial IAM products are acquired or restructured, institutions may face shifting support models, changing roadmaps, or new licensing requirements, adding long-term risk and uncertainty.

While commercial solutions are capable of supporting identity needs in higher education, they are often not optimized for the complexity, decentralization, and extended lifecycle requirements that define the sector. Institutions evaluating IAM options should consider not only immediate functionality, but also the system's ability to support academic governance models, staffing realities, and federated service needs well into the future.

The "total cost" illusion: What commercial IAM quotes don't show you

Commercial IAM solutions often appear affordable at first glance. Their pricing pages feature clean, predictable per-user licensing models that suggest scalability, transparency, and simplicity. But this surface-level pricing conceals a far more complex and costly reality that many higher education institutions discover only after implementation begins.

IAM in higher education is not just about licensing a product. It requires deep integration with institutional systems, support for complex governance structures, and ongoing adaptation to academic lifecycle changes. When commercial solutions are evaluated solely on license cost, institutions risk underestimating the true scope and expense of the effort.

Incomplete pricing models

Most commercial IAM offerings publish their SaaS licensing costs and little else. What's left out are the implementation fees, third-party consulting engagements, and additional service subscriptions often required to achieve a minimally viable deployment in a higher education environment.

These hidden costs can include:

- Configuration and customization services
- Delegated administration enablement
- Federation support and middleware
- Role and attribute policy modeling
- System integration with student information systems (SIS), LMS platforms, HR systems, and more

For higher ed, these are not optional extras. Rather, they are foundational needs in a higher ed context, and they typically fall outside of standard licensing agreements.

Hidden implementation burdens

Unlike purpose-built solutions that include implementation guidance, many commercial IAM products rely on a network of third-party system integrators. For institutions, this introduces not just additional cost, but coordination complexity and risk.

Implementations can run well into seven figures and take a year or more to complete. Delays are common when institutions underestimate the internal effort required: identity data mapping, business process redesign, access policy negotiation, and testing all require dedicated staff time. And many institutions begin IAM projects already operating with constrained IT teams stretched across other mission-critical initiatives.

Some commercial IAM vendors mandate the use of proprietary or fixed cloud infrastructure, limiting an institution's architectural flexibility and choice of hosting environment. In contrast, while Navigate is most commonly deployed on AWS as a managed service, institutions retain the option to host it themselves on-premise or in their preferred cloud environment.

The cost of scaling users

Commercial IAM pricing models frequently penalize institutions for growth. Adding applicants, alumni, or guest users can dramatically increase recurring licensing fees or may be unsupported altogether. Yet these populations are essential to the academic mission.

Alumni often maintain lifelong relationships with their institutions. They may reengage as graduate students, become donors, or serve in adjunct roles. Excluding them from IAM systems undermines the institution's ability to manage these relationships effectively. Including them under a per-user pricing model may require six-figure annual investments that offer no additional functional benefit.

Why price isn't everything

For higher education, identity is a continuity asset that far outweighs most security concerns. Institutions need to maintain identity histories across decades, support complex user journeys, and facilitate trusted access at every stage. Licensing models that treat every identity as a cost center ignore this long-term value.

Moreover, the complexity of academic environments means that implementation costs often exceed licensing costs, making upfront pricing a poor predictor of total investment. Institutions should evaluate IAM solutions based on long-term cost of ownership, sustainability, and strategic fit, not just initial price tags.

A better way to price: total cost evaluation

To support more accurate evaluation, institutions should assess IAM platforms using an end-to-end cost checklist that includes:

- SaaS or software licensing
- Internal and external implementation costs
- Long-term support and maintenance
- Integration with institutional systems
- Federation capabilities
- Delegated administration and governance support
- Guest, applicant, and alumni account handling
- Scalability and extensibility over time

Only by accounting for these factors can institutions make informed decisions that reflect the full scope of IAM responsibilities and avoid costly surprises mid-project.

A Higher Education-native alternative: Navigate IAM

Rather than retrofit commercial IAM platforms to meet the unique demands of higher education, institutions increasingly seek solutions built from the ground up with academic realities in mind. Navigate IAM is one such solution, featuring modular, cloud-based identity and access management rooted in open-source tools and designed specifically for higher education.

Developed and supported by Unicon, Navigate leverages the InCommon Trusted Access Platform (ITAP) stack, including Shibboleth for federated single sign-on (SSO), midPoint for identity lifecycle and governance, and Grouper for group and policy-based access control. Each of these components was created and refined through active collaboration with higher education institutions, making them well-suited to the governance models, identity lifecycles, and scale of academic environments. Unicon serves as a managed service provider, ensuring their secure deployment, configuration, and maintenance in alignment with higher education best practices.

Higher education-native from the ground up

Navigate IAM incorporates key standards and tools developed within the academic community, including:

- **Shibboleth:** A leading open-source Identity Provider (IdP) that supports SAML for federation with trusted frameworks such as InCommon and eduGAIN, as well as CAS and OpenID Connect (OIDC) positioning institutions for both current and emerging federated identity use cases.
- **midPoint:** A robust identity management and governance platform offering policy-driven provisioning (rules that automate access based on attributes and roles), role management, and auditing.
- **Grouper:** A group and access management solution that supports dynamic role hierarchies, delegated administration, and access policy enforcement.

These tools are deeply integrated and supported as a managed service, reducing the operational burden on internal teams while preserving flexibility and transparency.

Navigate's architecture is cloud-native and built on AWS, with deployment models that prioritize security, fault tolerance, and scalability. Institutions can review the full architectural diagrams to understand how Navigate separates identity services, protects sensitive data, and ensures high availability across distributed environments.

Modular, flexible, and transparent

Unlike monolithic commercial IAM solutions, Navigate allows institutions to adopt only the components they need. For example, a university might initially implement Shibboleth for federated SSO, then phase in midPoint and Grouper as part of a longer-term governance strategy. This modularity allows institutions to align IAM investments with readiness, staffing, and budget cycles.

Institutions may already rely on commercial tools for single sign-on (SSO) or directory services. Navigate can integrate with these existing systems to provide the governance, lifecycle management, and federation capabilities that are often missing from commercial IAM platforms. This hybrid approach allows institutions to maintain continuity while incrementally shifting toward an IAM model designed for the unique requirements of higher education. With Navigate, institutions retain control over architecture choices, integration strategies, and deployment timelines.

Importantly, Navigate is fully transparent. There are no black-box components, no proprietary protocols, and no constraints on how institutions can extend or adapt the system. Source code, data models, and configuration logic are all accessible.

Deep implementation partnership

Unicon offers full implementation and support services for Navigate IAM, with a team that brings decades of experience working exclusively in higher education. This includes:

- Project management and discovery facilitation
- Technical implementation of midPoint, Shibboleth, and Grouper
- Policy guidance for access control and governance
- Integration with SIS, LMS, HR, and research systems
- Ongoing monitoring, upgrades, and support

Unicon's role extends beyond installation. The same team that implements Navigate also helps institutions configure policies, train stakeholders, and adapt to future needs.

Transparent pricing, sustainable support

Navigate departs from per-user licensing models. Institutions are not penalized for scaling identity populations, supporting alumni, or expanding access to applicants and guests. Instead, pricing is based on services provided (e.g. implementation, managed hosting, and optional add-ons) with clear, up-front estimates.

Support needs also decline over time. As identity policies stabilize and workflows mature, institutions often see a reduction in complexity, support hours, and maintenance interventions, leading to a lower total cost of ownership over the long term.

Built *for* higher education and *by* higher education

Navigate is not a corporate product repurposed for campus use. It is grounded in open-source projects created by and for the academic community, with contributions from institutions across the globe.

This heritage ensures that the platform reflects higher education priorities like federation, data sovereignty, research collaboration, and decentralized governance. Institutions adopting Navigate join a broader community of practice and benefit from shared expertise, tested patterns, and ongoing innovation.

IAM for Higher Ed requires a different playbook

For decades, commercial IAM platforms have defined best practices for centralized, corporate IT environments – structured organizations with stable job roles, top-down access policies, and singular governance authority. These assumptions, however, don't align with the realities of higher education, where decentralized governance, fluid identities, and academic collaboration are the norm. Applying corporate IAM logic in this context often introduces unnecessary complexity, cost, and risk.

Higher education needs a different playbook that reflects the sector's unique identity patterns, federated collaboration models, and decentralized governance structures. This requires more than superficial feature parity. It calls for systems that are:

- **Purpose-built** to accommodate overlapping roles, temporary affiliations, and academic calendars
- **Flexible** enough to support distributed policy enforcement and delegated administration
- **Federation-native** to meet research collaboration and inter-institutional access needs
- **Scalable** to accommodate lifelong identity relationships and multi-million-user populations
- **Transparent and extensible,** so institutions can adapt to evolving security, compliance, and organizational needs

Navigate IAM offers this purpose-built alternative. Built on core components of the InCommon Trusted Access Platform and delivered by Unicon, Navigate aligns identity architecture with the structural and operational realities of higher education. It enables institutions to move beyond retrofitting corporate tools and toward a model that is sustainable, interoperable, and institutionally owned.

Navigate helps institutions reclaim control over identity strategy as both a security layer and a critical enabler of teaching, research, and community engagement.

Ready to rethink IAM for higher education?

Identity and access management is a strategic, operational, and cultural challenge. It demands solutions built for the unique realities of academic institutions.

If your current IAM platform feels too rigid, fragmented, or costly to adapt, you are not alone. Institutions across the country are re-evaluating their approach to ensure that their IAM systems reflect on how HigherEd truly works.

Whether you're exploring a full IAM replacement, considering a hybrid deployment, or simply want to benchmark your current strategy, we can help. Contact us at info@unicon.net or visit https://navigate-iam.com for more information.

Explore how a higher education-native solution can reduce friction, support compliance, and deliver the flexibility your campus needs.