

MICROSOFT IDENTITY MANAGER TRANSITION · HIGHER EDUCATION

MIM to Bravura Identity: Technical Comparison

How Microsoft Identity Manager capabilities map to Bravura Identity. Why Entra ID Governance does not cover the same ground. What a phased migration involves.

Jan 12, 2021

Mainstream support ended

Jan 9, 2029

Extended support ends

April 2026

Service Pack 3: no support extension

— THE EVALUATION WINDOW

Microsoft Identity Manager has reached the end of its active development cycle. Your institution needs a platform decision now, not in 2027 or 2028.

Mainstream support for Microsoft Identity Manager ended January 12, 2021. Extended support delivers security patches only, through January 9, 2029. No new features have shipped since 2021. Microsoft Service Pack 3 (April 2026) addressed platform compatibility and Azure SQL support; it did not extend support dates or introduce identity capabilities.

Higher education procurement takes two to three years. An institution that begins evaluation in 2027 chooses under deadline pressure. An institution that begins in 2026 chooses on its own terms.

— WHY ENTRA ID GOVERNANCE IS NOT ENOUGH

You will use Microsoft Entra ID. You will still need Bravura Security for what it does not cover.

Microsoft recommends Entra ID Governance as the path forward from MIM. For purely cloud and Microsoft-centric environments, that recommendation is sound. Higher education runs decentralized, heterogeneous environments. The same constraint that limited MIM applies to Entra ID: both platforms are Microsoft-centric. Neither covers the on-premises and non-Microsoft governance work your institution requires.

Cloud-first provisioning

Entra ID Governance is cloud-first by design. On-premises provisioning runs via the ECMA Connector Host agent, with limited depth in legacy system provisioning.

Partial separation of duties

Hierarchical separation-of-duties scenarios are not fully supported natively. Advanced SoD requires third-party partnerships.

No multi-affiliation lifecycle

Lifecycle automation is keyed to per-user HR attributes. A person who is student, employee, and alumnus has no native way to carry separate affiliations with their own start and end dates.

FERPA and GLBA

Verify adequacy with your compliance team before selecting Entra ID Governance as your sole governance platform.

The market pattern. Cloud-first platforms cover your cloud and Microsoft estate well. Broad coverage of your on-premises and non-Microsoft systems is what sets a platform apart.

CAPABILITY COMPARISON

Here's what Microsoft Identity Manager does today, mapped to Entra ID Governance and Bravura Identity across six governance dimensions relevant to higher education.

Capability	Microsoft Identity Manager	Entra ID Governance	Bravura Identity
Connectors and provisioning to non-Microsoft and on-premises systems	Built-in connectors for LDAP, SQL, SAP, Oracle, IBM, and more. ECMA2 for additional systems.	Cloud-first. On-premises provisioning via ECMA Connector Host agent. Less depth in legacy system provisioning than a purpose-built connector library.	Broad out-of-the-box connector library across Microsoft and non-Microsoft systems. A standard Python connector SDK and customer-verified connectors extend it. Higher education adds a standard Banner pattern. Custom MIM connectors may need equivalent work on Bravura Identity.
Joiner, mover, leaver automation across heterogeneous systems	Supported. Custom .NET rules extensions or PowerShell connector scripting typically required for non-Microsoft targets.	Cloud-app and HR-driven lifecycle workflows. Includes on-premises AD. Limited reach across heterogeneous non-Microsoft systems.	Rule-driven automation across the full environment on your migration timeline.
Reconciliation of out-of-band access changes	Scheduled sync cycles only.	Agent-based periodic sync. Real-time detection of out-of-band changes requires additional configuration.	Automated reconciliation built in.
Role and entitlement modeling for decentralized institutions	No native role model. Limited role hierarchy. No native affiliation construct.	Single-tier role model. Lifecycle driven by per-user HR attributes. No affiliation construct.	Multi-tier role hierarchies and affiliation modeling built for complex, decentralized institutions.
Separation of duties for FERPA and GLBA	Not native.	SoD enforcement during access requests and reviews. Hierarchical and relationship-aware SoD not fully supported natively. Advanced SoD relies on partner tools.	Advanced SoD controls built for institutions with FERPA and GLBA access control obligations. Verify adequacy with your compliance team.
Access certification and audit retention	No certification workflow. Basic audit logs.	Access reviews and certification available. Audit log retention 30 days with P1/P2; longer retention requires export.	Certification plus complete audit trails with retention controls.

Comparison based on published Microsoft and Bravura Security product documentation. FERPA/GLBA adequacy: verify with your compliance team.

A PHASED MIGRATION APPROACH

A phased approach manages risk and maintains continuity of identity governance during transition.

The January 9, 2029 support deadline sets the outer boundary. Within it, your environment complexity and procurement cycle set the pace.

1	2	3
Month 1	Complete before January 9, 2029	
Month 36		
PHASE 1 Discovery and Architecture Review Months 1 to 3	Map all systems currently connected to MIM. Document provisioning rules, sync schedules, and any custom PowerShell logic. Identify LDAP, SQL, SAP, Oracle, PeopleSoft, and non-standard connectors. Establish the connector requirements for Bravura Identity. A 45-minute session with a Bravura Identity specialist starts the review. It captures your standardized environment details for a structured fit assessment. Any non-standard scope or connectors get follow-up research before the written assessment is final.	
PHASE 2 Pilot Months 4 to 9	Deploy Bravura Identity for a subset of your environment: one directory type or one organizational unit. Validate connector behavior, joiner-mover-leaver rules, and separation-of-duties enforcement. Run MIM and Bravura Identity in parallel for the pilot scope. Define rollback criteria before the pilot begins.	
PHASE 3 Production Migration Months 10 to 36	Migrate production workloads in priority order: highest-risk systems first, then breadth. Decommission MIM sync agents as each workload is validated. Complete migration before January 9, 2029, the date Microsoft Identity Manager extended support ends and security fixes stop. Workloads not yet migrated keep receiving those security patches until then.	

WHERE BRAVURA IDENTITY FITS BEST

Bravura Identity fits best where governance and provisioning extend beyond the Microsoft stack. That includes institutions with on-premises systems, non-Microsoft directories, multi-directory environments, or hierarchical separation-of-duties requirements. If your institution runs a mix of Microsoft and non-Microsoft systems, Bravura Identity governs the full environment on one platform. **Entra ID remains your cloud and Microsoft foundation, and Bravura Identity governs the systems around it.**

NEXT STEP

Request an Architecture Review

The review starts with a 45-minute session with a Bravura Identity specialist. No sales presentation. It begins a structured fit assessment for your environment.

The session captures your environment details. Your written fit assessment and phased migration outline follow after any non-standard scope is reviewed.

THE REVIEW COVERS

Connector requirements for your directory types

Governance and SoD requirements

Migration sequencing

Risk assessment

bravurasecurity.com/identity-governance-solution-for-higher-education