Saviynt

Case Study

UniSC Establishes a Governed, AI-Ready Identity Foundation Across a Complex University

How the University of the Sunshine Coast replaced fragmented, manual identity processes with a cloud-based governance platform — improving access consistency, reducing helpdesk load, strengthening compliance, and laying the groundwork for AI and non-human identity security.



University of the Sunshine Coast Australia

Overview:
A 32-year-old Queensland university, with campuses from the Sunshine Coast to Moreton Bay, producing job-ready graduates and applied research, and working closely with local industry, government and community partners.

Headquarters:
Sunshine Coast, Queensland, Australia

Industry:
Higher Education

Segment:
Public University

Saviynt Capabilities:
- Identity Governance & Administration (IGA)
- AI-Enabled Identity Security
- SOCI Compliance

A Growing University With a Complex Identity Challenge

The University of the Sunshine Coast is a young, fast-growing public university operating across multiple campuses in southeast Queensland. It supports students, academic and professional staff, researchers, contractors, technology partners, and visitors — all with different access needs, different lifecycles, and different risk profiles. Behind that community sits a technology environment that has expanded organically across more than thirty years, accumulating more than 260 applications spanning cloud services, on-premises systems, and specialist research platforms.

For Niranjan Prabhu, Chief Information Officer at UniSC, the scale and diversity of the identity challenge was the defining issue. As he put it,

Every identity group had its own lifecycle and its own risk profile: students enrolled for semesters or years, staff changed roles or departed, contractors and visitors needed time-bounded access, and an increasingly large population of non-human identities — service accounts, automated agents, and AI-enabled tools — was entering the environment alongside the humans they supported. Ensuring every identity had the right access, for the right period, with a clear audit trail had become impossible to sustain through manual processes alone.

> **Being a university, we have a complex set of identities. We have a huge turnover of identities because students join in thousands and leave in thousands every year. We have different types of identities — staff, students, researchers, and partners, and visitors. Each of those identities require a different type of access to our systems, services, and timelines.**
>
> — **Niranjan Prabhu**, CIO, University of the Sunshine Coast

Fragmented Processes, Limited Visibility, and Growing Risk

UniSC's identity environment reflected the reality of a university that had grown rapidly without a unifying governance layer. Systems and processes had evolved independently, resulting in access provisioning methods that differed across applications, teams, and identity types. As Niranjan described it, the university's digital ecosystem had grown over thirty years, introducing its own complexities — in terms of access methods, whether manual or digital, how access was provisioned, and whether it was efficient enough to manage the complete lifecycle.

The practical consequences were felt most acutely when staff joined or changed roles. Activating access across the university's core platforms — wireless, local area network, Microsoft ecosystem, and line-of-business applications — required separate processes for each system, coordinated across different teams. In Niranjan's words:

UniSC's identity environment reflected the reality of a university that had grown rapidly without a unifying governance layer. Systems and processes had evolved independently, resulting in access provisioning methods that differed across applications, teams, and identity types. As Niranjan described it, the university's digital ecosystem had grown over thirty years, introducing its own complexities — in terms of access methods, whether manual or digital, how access was provisioned, and whether it was efficient enough to manage the complete lifecycle.

The practical consequences were felt most acutely when staff joined or changed roles. Activating access across the university's core platforms — wireless, local area network, Microsoft ecosystem, and line-of-business applications — required separate processes for each system, coordinated across different teams. In Niranjan's words:

> **When a staff member joins, they need access to their wireless, our local area network, our Microsoft ecosystem, and then there are line-of-business applications. None of those accesses are consistent. Some have to be raised with the IT service desk, some need to be manually informed. In the past, we used to provide access based on 'such and such a person' — but that person might have been in the university for years. There was no continuous monitoring. The inherent permissions would be acquired by a new person without checking whether that person should have access.**
>
> — **Niranjan Prabhu**, CIO, University of the Sunshine Coast

Consistency, Efficiency, Compliance, and an AI-Ready Roadmap

After a formal tender process, UniSC selected Saviynt on the basis of three primary business drivers: consistent access provisioning across all systems, a more efficient and less manual approach to identity lifecycle management, and the compliance and audit visibility needed to meet regulatory obligations.

Forward capability on AI-enabled identity security was the third decisive factor. UniSC was not looking for a platform to address only its current state. As Niranjan explained:

> **We also have a future roadmap where we will be using the AI-enabled capability and self-service capabilities. That is where we saw Saviynt as one of the key products that can enable that journey as part of our digital transformation.**
>
> — **Niranjan Prabhu**, CIO, University of the Sunshine Coast

Saviynt gave UniSC a foundation that addressed immediate compliance needs while remaining aligned with where the broader identity security market was heading.

From Manual Complexity to a Governed Identity Lifecycle

UniSC's identity transformation began with a detailed mapping of the existing environment — cataloguing access requirements across priority applications, engaging application owners to document provisioning processes, and defining a target governance architecture. The platform foundation was established first, followed by progressive onboarding of priority applications beginning with the highest-risk systems critical to SOCI compliance.

The scale of what that mapping revealed was itself a finding. As Niranjan described it, when they started across their 260+ applications, it was hard to find out who had access to which system and who should have access — mainly because systems and services had grown organically, with a lack of documentation, inconsistent processes, and inconsistent methods of applying security to key resources.

The journey required mapping access requirements, engaging application owners, identifying provisioning processes, and defining the to-be state collaboratively with key stakeholders.

Establishing Standard Workflows and Business Ownership

The initial phase replaced ad hoc, application-specific processes with standard workflows and clear business ownership. Saviynt was integrated with UniSC's core systems, establishing the joiner-mover-leaver lifecycle as a governed, repeatable process rather than a collection of manual interventions. Application owners were given direct visibility into the identities accessing their systems and clear accountability for approving and reviewing access.

Enabling Day-One Access and Self-Service Provisioning

> **Each of the system owners can now see which identities have been provisioned, and we have a way of tracking them with regular checks. We are also providing access approval back to our end users so they can provision without IT's involvement. End users are provisioned to those key systems on day one — at the right level, with the proper access, for the proper timeline.**
>
> — **Niranjan Prabhu**, CIO, University of the Sunshine Coast

Efficiency, Compliance, and a Foundation Built to Scale

~20%	Weeks → Day 1	SOCI
Reduction in helpdesk tickets(early stage, 7 apps)	Time-to-access for new staff on onboarded systems	Critical infrastructure compliance supported

The improvements in access speed have been immediate. Provisioning that previously required multiple coordinated tasks across multiple teams — often stretching over weeks — now happens within the same day for onboarded systems. Access reviews have seen an equally significant shift: what previously took several weeks is now instant, supported by automated review cycles and a central audit trail showing which identities retain access and which have been removed.

The reduction in manual provisioning work has freed IT staff for higher-value activities, with helpdesk ticket volume measurably declining.

That shift in audit readiness — from manually assembled evidence to a centrally maintained audit trail — directly strengthens UniSC's position against its SOCI regulatory obligations and internal governance requirements.

> **The federal government has the Security of Critical Infrastructure as a requirement for all universities. As part of our security architecture, we use Saviynt to provide that kind of assurance, so that we can monitor, report, and be compliant with those requirements. It is easier to provide the evidence now with Saviynt deployed, compared to what we used to provide — manual evidence assembled across multiple systems.**
>
> — **Niranjan Prabhu**,
> CIO, University of the Sunshine Coast

AI and Non-Human Identities: Governance for What Comes Next

AI adoption at UniSC spans three domains — operations, teaching and learning, and research — and the university has established a cross-functional AI task force to govern its responsible deployment across each. For Niranjan, the governance of AI begins with identity: ensuring that the tools, agents, and automated integrations entering the environment are subject to the same ownership, access controls, and lifecycle management as human identities. Whether it is a service account or an account used by AI, he argued, it needs the same amount of rigour, visibility, and compliance as human identities — to make sure it is doing the right thing and providing the right information to the right person at the right time.

The risk of AI tools entering the environment undetected — through student or researcher adoption of consumer services, or through AI capabilities embedded in existing platform upgrades — is a concern Niranjan raised:

On the opportunity side, UniSC sees AI-powered identity capabilities as a path toward continuous, risk-based governance. AI can assist in providing context-based access reviews automatically and serve as a continuous monitoring agent — seeing and tracking unusual combinations of access much faster and more efficiently than human reviewers, while flagging issues for human decision rather than replacing human oversight entirely.



AI is fast-evolving. It enters our institution in many shapes and forms — through services that use AI, or through tools our students and researchers bring in that may not be visible to us. Preparedness is what I'm most concerned about.

— **Niranjan Prabhu,**
CIO, University of the Sunshine Coast

A Strategic Partnership Built on Platform Capability and Shared Expertise

For UniSC, the value of working with Saviynt has been both the platform capability and the depth of the professional engagement. The Saviynt professional services team brought cross-industry experience across multiple regulated environments and applied it directly to UniSC's specific requirements — guiding implementation to an industry-based standard rather than delivering a generic deployment.

That two-way relationship — contributing the higher education perspective to Saviynt's product roadmap while gaining early visibility into emerging capabilities — positions UniSC to stay ahead of the governance challenges that AI adoption and non-human identity growth are introducing.

> **Participating in Saviynt's Strategic Advisory Board provides insight into how the product is being developed to address the future — the roadmap capabilities being introduced into the platform. By participating, we can provide input on where UniSC is heading in its own transformation agenda, and make sure the features and capabilities being introduced cater for our sector. Having that early insight helps both ways — it ensures the investment we made in Saviynt is providing that benefit, and it provides insight to the product team on what the education sector is looking for going forward.**
>
> — **Niranjan Prabhu**, CIO, University of the Sunshine Coast

Looking Ahead: Embedding Identity Security as a University-Wide Capability

UniSC's roadmap is focused on extending consistent governance to every application and identity type in the environment — onboarding more applications, increasing automation across the full joiner-mover-leaver lifecycle, and applying the same standards to non-human and AI identities as to human ones. The goal is to move identity security from a major transformation program into a sustainable, embedded university capability.

The stakes of getting this right — and the risks of not — are clear. Without proper identity security, Niranjan argued, the risk could be significant: identity theft, access by actors who should not have it, failure to meet compliance and regulatory requirements, and insufficient visibility to act during major security incidents. The reputational, financial, and trust implications for a university — with both internal and external stakeholders — make it a priority that goes well beyond IT.

> **We have started this journey to make sure our technological digital assets are provisioned seamlessly to the users who need them at the time they need them. As we expand our footprint and adopt new services, we want the same consistent approach to the way we provision identity, manage identity, and respond to identity-related incidents. This is where we are looking at Saviynt as a core partner — as and when our technology footprint changes, whether it is AI, automation, or even quantum technology — so that we are better prepared and ready for the transformation ahead.**
>
> — **Niranjan Prabhu**, CIO, University of the Sunshine Coast

About Saviynt

Saviynt is the identity security platform built to secure the modern enterprise. With Zuma, its complete AI security platform, Saviynt helps organizations build, run, and scale AI with confidence. The world's leading brands trust Saviynt to reduce risk, improve visibility, and support compliance while enabling business agility.

Saviynt

Headquarters
1301 E El Segundo Blvd,
Suite D El Segundo, CA 90245
United States

310.641.1664
info@saviynt.com
www.saviynt.com