Quantum Secure and Higher Education

ABOUT OUR CLIENT

Our client, a private research university in the southwestern United States with two satellite campuses, has over 11,000 students and 1,000 academic staff members on its three campuses.

CHALLENGES AND REQUIREMENTS

Managing over 12,000 student, faculty and staff identities as well as the large number of contractors, vendors, and visitors that access the campus daily is a difficult task. The university faced the difficult challenge of not only managing this large number of identities with different risk profiles, but also managing each identity's physical access requirements for campus facilities such as residence halls, classrooms, laboratories, cafeterias and libraries. Adding an additional level of complication was that not only are these access zones managed by multiple physical access control systems (PACS), but the university also utilizes multiple authoritative systems in these same facilities as part of their physical security infrastructure. These additional systems include a Human Resource Management System (HRMS) for faculty and administrative staff, Admissions and Records Systems for students, Parking systems and Residency Management Systems (RMS). With all of these challenges and a limited security budget, it was a difficult job for the university's physical security team to maintain a safe learning environment.

The key challenges faced by the university lie in the inherent complications of the previous systems and processes for managing physical identities and their access:

Lack of Consolidated View Into the Identity Population and Their Physical Access Rights

The university has multiple authoritative systems to enroll and manage identities such as, student enrollment systems, HRMS, RMS, and parking systems as well as multiple access control systems to manage credential and physical access information for these identities. Unfortunately, none of these systems provided a consolidated view of all these physical identities, their credentials and access. They lacked a consolidated view of the entire identity population at the university.

Silos of Identity Systems – Physical, Logical and Other Authoritative Systems with Limited Integration

The complication described above was aggravated because of the multiple identity-based systems which in turn have multiple stakeholders. These systems store data for the same person, but due to the lack of proper integration data exchange happens through manual interactions. These solutions also had limited or no integration with authoritative and logical security systems. As a result, there were huge operational inefficiencies, delays and a high state of risk to potential security exceptions.

Manual Enforcement of Security Policies Related to Physical Access Control

The university's physical security systems managed identity, credential and access data but lacked the capability to automate the policies and processes of managing security for people and property. This caused a great deal of manual intervention by the physical security team resulting in delays and manual errors and also requiring a high level of effort from the team.

COLOR ID
Toll Free: 888.682.6567
ph: 704.987.2238
fx: 704.987.2240
www.ColorID.com

THE QUANTUM SECURE SAFE SOLUTION

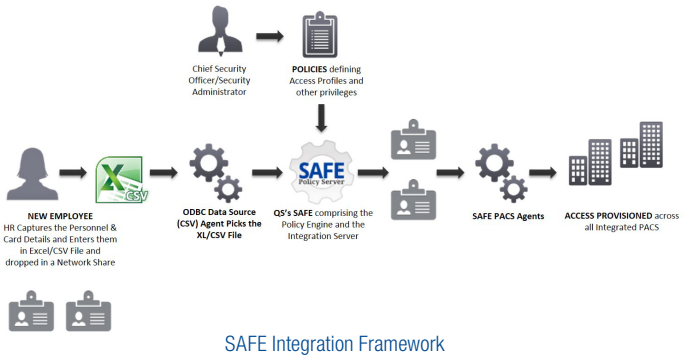
The university selected Quantum Secure's SAFE Physical Identity and Access Management Solution to provide them with a comprehensive view of their physical access-related operations and automate their existing manual processes associated with the access and identity lifecycle management resulting in faster processing time and better audit controls.

Provide Integration and Interoperability of the Siloed Physical Security System

SAFE provides ready-to-use connectors (agents) which integrate with the external disparate PACS present at the university and authoritative systems (HRMS, Parking, Admission and Records) to provide a common centralized security platform. This ensures that the security system is up and running within hours and minimized operational delay due to project implementation. Also with the ability to communicate across devices and systems, SAFE delivers the university with a unified comprehensive view of their security and provides seamless processing of identity information from the PACS to SAFE.

Automate the Entire Physical Identity Lifecycle Management

SAFE also allows the university to design custom policies based on their security processes and uses these policies to automate workflows related to identity lifecycle management such as access provisioning / termination process and automated rules and workflows for access rights management.



SAFE Integration Framework

Comprehensive Reporting

SAFE provides the university with a robust and full-featured reporting capability that supports workflow embedded, scheduled, and ad-hoc reporting of identity and physical access events and activities. SAFE provides key reports and dashboards for on-boarded identities, their access details and badging activities across multiple views for the university to make appropriate operational decisions and prevent any possible threats. Administrators can display this information as a user configurable dashboard to graphically display such information in an at a glance view as well as configure reports to be sent to SAFE users based on events/triggers or scheduling defined in the policy engine.

End-to-End Badge Management

SAFE helps issue secure smart card credentials to both ensure secure access to university facilities and thwart the possibility of counterfeiting ID cards. ID cards used at the university are dual-technology – mag stripe and smart card. SAFE encodes as well as decodes mag stripe cards and prints barcodes on the cards to prevent counterfeiting. Similar to attribute-based access provisioning, SAFE allows automatic association, issuance and printing of a university pre-approved badge template based on the attribute(s) of the identity. SAFE also allows the university to manage badge policies such as setting up a badge expiry date and automating the renewal cycle when required.

Watch List Manager

The SAFE Watch List Manager is used to verify identities across all affiliations to reduce the risk of allowing a known high-risk person access to university facilities. The SAFE Watch List Manager compares identities to one or more watch lists. If an identity is flagged, a reviewer is notified. If they do not approve the identity, then SAFE will not allow clearances to be assigned or badges to be printed for the identity, ensuring unauthorized identities don't get access to the university's premises.

BENEFITS

The SAFE Solution at the university has replaced the manual processes associated with personnel on/off-boarding, card issuance, access assignments, provisioning in PACS at the university such that new personnel can be on-boarded and operational in minutes rather than days/weeks. SAFE ensures up to a 90% reduction in manual interventions for the processes related to identity management, which saves the university a huge sum in annual operation costs.

To summarize, the overall benefits are as follows for the university utilizing SAFE Software from Quantum Secure:

- **Safer Premises:** With SAFE, providing centralized administration of all access management processes and watch list checks, the security team at the university now has a comprehensive, unified view of their entire physical operations. This ensures that unapproved identities should not be able to access university premises.
- **Enhanced operational efficiencies:** With SAFE providing automation of manual tasks and system interoperability, identity access requests are approved within minutes without any delay; improving their operational efficiencies
- **Substantial Reduction in Operation Costs:** SAFE provides the university with immediate operating cost reduction by automating the access management process.

COLOR ID
ph: 888.682.6567
fx: 704.987.2240
www.ColorID.com