

How a Leading Hospital Group Unified Identity Across Its Clinical and Business Applications with Cross Identity

Automated joiner, mover and leaver processes, single sign-on for web, mobile and thick-client applications, governed access, and a customer identity layer, all on one converged platform.


6,000

workforce users

5,000

patient users

54

integrated applications

THE CHALLENGE

A round-the-clock workforce changes daily through joiners, rotations, transfers and exits, while each application managed its own users and IT teams handled accounts manually.

Fragmented identities	The same person existed separately in AD, SAP, the HIS/EHR and other apps.
Lingering access	Former staff and contractor accounts stayed active, putting patient data at risk.
Too many passwords	Separate logins for every app slowed care and drove help desk volume.
Weeks of audit preparation	No reliable way to find privileged access or produce evidence for regulators.

WITH CROSS IDENTITY

The group selected Cross Identity's converged platform for identity governance, access management and customer identity. The results:

HRMS AS THE SOURCE OF TRUTH

Identities no longer fragmented

One HR-based record per person, trusted everywhere.

AUTOMATED JOINER, MOVER, LEAVER

Access follows the person

Ready on day one, updated on transfer, removed on exit.

SINGLE SIGN-ON FOR EVERY APP

One login replaces many

One MFA sign-in for web, mobile and desktop apps.

HOMEOWN APPLICATIONS

No application left behind

In-house apps get the same controls as commercial ones.

IDENTITY GOVERNANCE

Audit-ready on demand

Requests, reviews and evidence in one place.

CUSTOMER IDENTITY (CIAM)

One secure front door

Secure sign-in for patients and partners.

BUSINESS OUTCOMES

Day-one productivity

Role-based access on the first shift; extra access in hours, not days.

Reduced security risk

Leavers lose access everywhere when HR records the exit.

Less clinician friction

One login across web, mobile and desktop at the point of care.

Audit readiness at scale

Evidence on demand, on a platform tested with 7 million+ records.

HOW CROSS IDENTITY DELIVERED THESE RESULTS

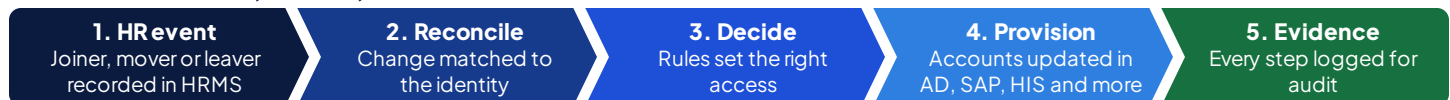
Process	Before Cross Identity	After Cross Identity
Onboarding	Tickets to each app owner; days to get AD, SAP and HIS access.	Ready on day one. A new hire in HRMS creates the identity and every birthright account before the first shift.
Role changes	Transfers added new access and rarely removed the old.	Access moves with the person. A transfer adds what the new role needs and removes what it no longer needs.
Offboarding	Exits ran on email chains; accounts stayed active long after the last day.	Gone everywhere in minutes. One exit in HRMS closes every connected account in a single logged step.
Sign-in	A separate password for every system, including SAP GUI and the HIS.	One login, every app. Clinicians sign in once with MFA to reach web, mobile and desktop apps.

THE SOLUTION IN DETAIL

Capability	What was deployed
HRMS source of truth	HR records reconciled and used to drive all downstream access.
Joiner, mover, leaver	Role, department and location drive access in AD, SAP, the HIS/EHR and the super-app.
Single sign-on	MFA to My Apps: SAML/OIDC, browser-extension SSO for legacy apps, thick-client SSO for SAP GUI and HIS.
Homegrown applications	SAML, OIDC and API sign-in; API and database connectors for provisioning.
Identity governance	Requests, certification, orphan and privileged account flags, SoD checks, audit trail.
Customer identity (CIAM)	Self-registration, OTP and social login, MFA and consent for patients and partners.

HOW IT RUNS, STEP BY STEP

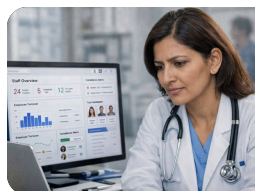
AUTOMATED JOINER, MOVER, LEAVER



ACCESS REQUESTS



ACCESS CERTIFICATION



SPOTLIGHT: HOSPITAL INFORMATION SYSTEM (HIS/EHR)

The HIS, the hospital's core clinical and operational system (the equivalent of an EHR), runs around the clock. Cross Identity integrated it for both SSO and IGA. **Access:** thick-client SSO from My Apps, with no separate password at shared workstations. **Governance:** accounts follow HR events and certification campaigns, so access to patient data matches each person's current role.

THE IMPACT

1 source of truth for all access	<1 hr to day-one access, down from 3 to 5 days	Minutes to revoke access on exit, down from days	~60% fewer password and access tickets
--	---	--	--

Figures are approximate, based on this deployment, and may vary by process and application.