



Overview

The client operates a network of hospitals through which they provide a wide range of healthcare services. They have grown to 24 hospitals, 7 heart centers and a network of primary care facilities across the country and an international hospital in the Cayman Islands. They provide advanced levels of care in over 30 specialties.

Industry: HealthCare

User: 13,500+

Application: 8+

Situation:

This Healthcare organization faced a huge turnover of nursing and paramedical staff as well as an increase in staff as it was experiencing a phase of high growth both in number of hospitals as well as staff. As a result, there was a frequent need to create new employee accounts and delete old accounts. In addition, staff work on shared workstations with shared logins for certain applications.

Challenge

- Multiple logins required to multiple applications
- Loss of productivity due to time spent logging into multiple critical applications
- Forgotten passwords required Helpdesk assistance
- Managing user accounts and permissions across different systems and applications was a laborious and ad-hoc without any proper processes in place
- Security and compliance issues arising from accounts being active even after employee separation

Requirements

- Single Sign on To Web Applications
- Password Self-Service
- Birthright Provisioning
- Automatic and Manual Provisioning
- Access Requests Management
- Role Management
- Orphan Account Management
- Access and Entitlements Recertification
- Automatic and Manual De-provisioning

Solution

- Password Self-service from any device, anytime and anywhere
- Multi-Factor Authentication
- Single Sign-On to all applications
- User Lifecycle Management
- Governance

Results

- Automated provisioning to target systems and applications
- User onboarding process with the birth right access is standardized
- Access Requests Management to automate creating, changing and revoking user accounts
- Proper termination process making sure that no unauthorized user has access to the applications post after their separation from the organization
- No orphan or unauthorized accounts
- With the ever-changing workforce, they have right access to the right users at the right time.
- Users rarely call the Helpdesk about forgotten passwords or locked accounts
- Users access all their applications without having to login to them every time

Benefits

- Increased Employee productivity
- Increased Helpdesk efficiency
- Enhanced User Experience
- Easily achieved the necessary Statutory and Regulatory Compliance as required for any Healthcare organization

For more information, visit <https://www.ilantus.com>

ILANTUS Technologies...the next generation Identity as a Service provider with a cloud based IAM platform. Our integration capability with both cloud and on premise thick client applications gives ILANTUS unique positioning among competitors.

Gartner rates us among the top 5 global IDaaS players and calls us a "Next Generation System Integrator" for Identity Management continuing to position ILANTUS in the niche vendor segment of Gartner's Identity and Access Management as a Service (IDaaS) Magic Quadrant.

The information contained in this document is highly confidential and privileged. No part of this document may be copied or circulated without express written permission from ILANTUS Technologies Private Limited. This document is for discussion purposes only.