Overview

With revenues of over 3.9 Billion USD, 15,000 employees and a fleet size of over 113 aircrafts, the client is a large airline that operates over 300 flights daily to 68 destinations worldwide.

Industry: Aviation
User: 5,000+
Application: Thick Client Apps (20+) and Web Apps (30+)

Situation

In the airline industry, this customer was committed to providing uninterrupted 24X7 service. However, it faced many challenges doing so. Non-tech employees faced password management issues which caused service interruptions. With many applications to access, users had trouble remembering all the passwords to all of their applications to open the applications quickly. When the customer enforced a stronger password policy to ensure security and comply with stringent compliance requirements, users added another layer on top of these passwords to remember which resulted in more forgotten passwords, locked accounts and more service disruption. The Helpdesk was now overburdened with password events which prolonged the service interruption on the user side and increased the work load on the service desk side. In addition, remote users such as the flight crew needed access to the Helpdesk around the clock, seven days a week because the Helpdesk had to be involved when they had password incidents out of the network and on their mobile devices.

Challenge

- Pilots, crew members and operations staff were facing the challenges of remembering passwords for different applications.
- Users were creating security issues from the use of different forms of password vaults, writing down their passwords and/or pasting their passwords on notes on their systems for their convenience.
- Considering a single sign on as a solution became unfeasible as there were no cost-effective SSO solutions that could handle the many thick client applications used daily.
- Security issues were causing compliance issues.
- Users were dependent upon the IT support Helpdesk to resolve password issues.
- Helpdesk needed to be available on holidays and off hours.
- Helpdesk costs kept increasing because of the demand place on the need for assistance.
- Productivity was suffering throughout the organization during these events for both the user and the Helpdesk

Requirement

Self-Service Password Reset and Account Unlock

- Self-Service Password Reset and Account Unlock
- Self-Service Password Management on Mobile Devices
- Ability to change or reset passwords while disconnected from the domain and office network
- Support for password management for different kinds of devices such as tablets and mobiles used by Pilots and airport staff
- Use of the same single password (SSO) to access all types of applications

Solution:

- Self-service solution for users to control password resets and unlock accounts
- Automated and fully scalable
- Ability to integrate with the HR system to auto register 28,500 users and enable all users to use the solution seamlessly as and when required by the management in a phased manner
- Reduced service desk assistance
- Ability to synchronize the Password Management System and existing HR software, PeopleSoft
- Password Synchronization to set the AD password to all target applications

Results

- Helpdesk Dependency: Significant decrease in password reset calls to the Helpdesk
- Highly Flexible Password Reset Policy: Multi factor authentication options such as SMS OTP, Soft-Tokens and Email OTP instead of the archaic Q&A based password reset methodology
- Reduced Sign-on time: Immediate access to all web and thick client applications with a Windows password that is synchronized across all applications
- Compliance and Reporting Capabilities: Strong auditing and compliance reporting capabilities which integrate with Security Information and Event Management (SIEM) solutions.

Benefits:

- SSO to web applications from any device
- Password Reset from any device at any time from any location
- Reduced password related Helpdesk calls.
- Increased User Convenience and Productivity
- High adoption rate due to enhanced User experience

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.