



Single Sign-On for Banking Sector

Overview

The client is a leading private sector bank with over 100,000 employees and a market capitalization of 45 Billion USD. The bank has over 4000 branches across over 2500 towns and cities and is also a leader in cross-selling of its products like Mutual Funds and Stocks.

Industry: Banking

Employees: 100,000+

Application: Web and Thick Client Applications
(over 700 combined)

Situation

The Bank has over 700 applications for their 100,000+ users that include web, thick client, smart client and Citrix applications. End users log into about 40 - 50 applications on a daily-basis and Administrators login to about 300+ applications on a regular basis.

This was a serious challenge for this enterprise. The user experience was a very frustrating and time-consuming affair, which resulted in tremendous productivity loss. Added to this, the enterprise had applications with shared credentials. End users across the company struggled with a high degree of inconvenience by having to login to multiple applications with different credentials.

Challenges

- Multiple logins required to different applications.
- Loss of productivity due to forgotten passwords.
- Increasing Helpdesk requests due to forgotten passwords and locked accounts which increased the Helpdesk cost.
- Security threats due to the use of shared credentials for certain applications.
- Lack of additional security for sensitive applications.
- Laborious manual process for granting access to key applications.

Requirement

- The solution should perform Single Sign-on to 700+ applications which includes web applications, thick client applications, smart client applications and Citrix applications.
- Multi-factor Authentication to improve security of some core banking applications.
- Shared ID credentials need to be hidden from the end users for security and yet still provide Single Sign-on access to multiple applications.
- Reduce Helpdesk calls related to password resets and unlocking accounts to the critical applications through the Single Sign-on dashboard without the need to login to these applications.
- Workflow for approval of access to Key applications.
- Time based access to privileged users.

Solution

A Single Sign-On solution was implemented for the Bank. Some of the key features of the solution are given below:

- Single-Sign On to all types of applications; web, thick client, smart client and Citrix applications.
- Built-in Password Vault for securely storing credentials of Non-AD authenticated and Non-Federated Applications.
- Multi-Factor Step-Up Authentication for sensitive applications.
- Auto-Launch with Single Sign-on to frequently used applications that are pre-configured based on users' role.
- Pre-configured Shared Credentials for users to Single Sign-on to all applications without providing any credentials.
- Automatic rearranging of application icons on the Single Sign-on Launchpad so that applications used more often, appear on top.
- Managers or Application Owners approve user's Single Sign-On access to an application.

Results

- Employees no longer need to fill in credentials and login multiple times to access each target application.
- Users rarely call the Helpdesk about forgotten passwords or locked accounts.
- Sensitive applications are more secure now with Step-up authentication along with the convenience of Single Sign-on.
- Users with Shared Credentials can use Single Sign-on to access applications without knowing the credentials for each application.
- Users can use Single Sign-on to access applications from remote locations without the need to connect to authorized networks.
- Higher security with a workflow based approval process to authorize applications for Single Sign-on users.

Benefits

- Increased employee productivity.
- Increased Helpdesk efficiency – Zero Password related calls
- Enhanced security to sensitive applications via multi-factor authentication along with the convenience of Single Sign-on.
- End users can access applications with Shared Credentials through Single Sign-on without knowing the application credentials.
- 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.

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.