

CASESTUDY

# Identity Management Solution for a leading global bank

### **About the Client**

The client is one of the largest banks in the world. Its data center located in Singapore manages over 53 business applications for the bank's operations in 76 countries. It is one of the largest data centers in Asia Pacific.

### **About the Vendor**

ILANTUS is a leading global solutions provider in the area of Identity and Enterprise Management. It has more than 100 man-years of experience and knowledge; implementing major projects for Fortune 1000 companies. ILANTUS strengths include a partner network of leading technology companies & a technology center in Bangalore to perform POCs, S/w development, troubleshooting, support and maintenance, thus providing excellent support and short turn around time for consultants on-site. ILANTUS works out of US, Singapore and India.

ILANTUS solutions include process re-engineering and automation of Identity and Enterprise Management practices; implementation & integration of appropriate technologies; integration of relevant tools with business applications, operations management, support and maintenance and also Consulting, Architecting, Implementation and support of IT Infrastructure & Enterprise Management Systems.

### **The Business Challenge**

The Singapore data center has more than 300 administrators and operators managing it. Because of the nature of their job, the system administrators have very high-level access to applications and servers. The data center management identified the present user management process as not adequate to support their security policy. A team of people studied the existing practices and identified following areas to be addressed by implementing a User Provisioning solution.

### **Requirements**

- To replace multiple access request approval processes with one process
- To automate the "Access request approval process" with an appropriate "Workflow System"
- To replace multiple forms for access request with one electronic form as a part of workflow system
- Implement an Integrated User Administration System for all the platforms
- Define responsibilities based on "Segregation of Duty" principle
- Implement maker and checker audit control as per the bank's Information Security Policy before a user is provided with access
- To manage all the accesses for one user with one virtual user ID
- To implement process and procedure to request, approve, create, revoke and delete user profiles as per the bank's Information Security Policy
- To integrate the access approval and User Management system
- To reduce the turn around time for access "request to provide" cycle
- Centralized maintenance of user profile to reflect the actual status of the user
- Design and implement "Role Based Access Control" system
- Implement and Alert and monitoring system for all User Administration Activities
- Implement simplified, effective report generation system for all User Administration Operations

## The Solution

Control SA Solution from BMC was implemented to address the above issues. The project involved a detailed pilot of the solution covering all platforms. Implementation was then carried out for full fledged user provisioning solution covering all user management activities, password self service and alerting system for identifying user management activities that violate security policies.

## Review of existing practices

ILANTUS reviewed the existing policies, procedures and access permission definitions on business application servers and sought to understand the activities of all the departments in the organization. The Singapore Data Center has 11 different platforms. The existing user administration practices for each platform & application were reviewed. In each of these areas, ILANTUS identified the problems that needed to be resolved.

## Implementation

Following the review, ILANTUS consolidated the existing policies and procedures and made necessary modifications and created new policies and procedures for certain areas, which were not covered by the existing policies. The necessary workflow process and procedures were developed. It was decided to implement processes, which would facilitate the data center by providing users access to business application and data on “need-to-know” basis. ILANTUS defined the roles and mapped the data requirement for the roles and provided the access using a workflow management and user administration tool. ILANTUS laid down a process to manage the policy updates and modifications using the workflow system.

## User Administration

ILANTUS implemented a user Provisioning solution on all servers and databases to create a single repository of User Profiles. User creation templates were developed to reduce entering information needed to create each user profile and speed up User ID creation. Job codes were then developed based on access as defined for roles created in the organization. This allowed User ID creation on multiple servers and databases to be completed with a single click. These User IDs on various systems and databases were linked to a single logical entity called the Enterprise User. This enabled easy identification of user's access to various servers and resources in the organization. It also allowed single-click deletion of User IDs on selective or multiple servers and databases thus ensuring that the directory of user profiles was always up-to-date.

Finally, resources on various servers and the corresponding user access permissions were defined. This simplified the method to define access permissions to various folders and directories. A Simple reporting tool was then created to extract the user administration database across all servers and databases. This enabled the Security Administrator to identify the tasks performed by each of the User Administrators. To wrap things up, passwords were synchronized and a single password for each user was deployed across all servers and databases. This reduced the number of password-reset requests. Password reset request is considered as unproductive request and hence required to be reduced to as minimum as possible. An alert and monitoring system was implemented. This sends SMS messages to mobile phones and emails to the User Administrators in case of any violation or interruptions.

As the entire system is non-intrusive, the impact on business was minimum. For example, in case of a system breakdown, the Administrator can go ahead and create a user profile directly on the server and provide access. The system updates the directory with this operation whenever it comes live.