

Case Study

Major Australian Bank Business Intelligence

The Customer

The Customer is a major Australian bank with a presence in all Australian states and capital cities, regional centres and overseas.



The Challenge

Growth and acquisitions over several years had created a number of challenges. The Customer's portfolio of applications was large and growing and the rate of introduction of new applications was expected to grow rapidly as business grew. The vast majority of these applications had their own unique security functions providing authentication and authorisation. This resulted in employees having to remember several different userids and passwords. Consequently a high number of password-related calls to the various application helpdesks were made each day. The proliferation of usernames and passwords was identified by the business as a significant impact to staff productivity.

The business was very keen to reduce the number of usernames and passwords that their staff had to remember in order to perform their jobs.

The Solution

The Customer conducted a review of their requirements and decided to implement an enterprise directory and an access management product to bring this situation under control. The first step was to implement the enterprise directory and populate it with entries for all staff and external parties who need to use the bank's internal applications.

The next step was to choose an access management solution. A thorough review of the available products led the bank to select the IBM Tivoli Access Manager for eBusiness product to address their access control requirements.

IBM Tivoli Access Manager for eBusiness

TAM for eBusiness provides authentication and authorisation functions for web-based (and other) applications. By using TAM for eBusiness, application developers no longer need to concern themselves with the development of authentication and authorisation code, as this can all be provided externally to the application by the TAM for eBusiness product. TAM for eBusiness provides a single authentication directory that can be used across multiple applications. It also allows an organisation to define and deploy its security policy (i.e. who is allowed to access what resources) to the Tivoli Access Manager policy enforcers. The policy enforcers ensure that only suitably authorised staff are allowed to access the bank's web-based applications



Services Delivered

During the systems implementation, the Customer recognised that they required assistance in the deployment, support and integration of their existing applications with TAM for eBusiness. They also recognised that their own support staff would require technical training and skills transfer. The Customer approached Senetas to provide high-level technical resources and training to assist with the implementation of TAM for eBusiness.

Senetas provided the following services during the project:

- Technical Consultancy – working with IBM and the Customer's technical staff to integrate Tivoli Access Manager with the Customer's enterprise directory. Assist



Case Study

Major Australian Bank Business Intelligence

Customer's technical staff with the resolution of problems in the Tivoli Access Manager environment;

- Design and Oversee Solution Build – in conjunction with the Customer's staff a detailed design for the build of the Tivoli Access Manager system was produced, validated and implemented across the Customer's testing and production environments;
- Develop and unit test customised password change and forgotten password functionality;
- Integration Solution Design – design and unit test the integration of a number of the Customer's applications into the Tivoli Access Manager environment;
- Training Program – deliver formal classroom-based training to the Customer's technical staff on the Tivoli Access Manager, as well as delivering "on the job" skills transfer.

The Benefits

The Customer has achieved the following benefits by implementing the TAM for eBusiness:

- Eliminated costs associated with the development, maintenance and administration of security specific code in new applications;
- Achieved a significant reduction in the number of userids and passwords that staff members must remember in order to perform their job functions;
- Reduced calls to helpdesks for password resets due to the provision of the self-service forgotten password function;

The Future

Senetas has continued to provide customised training as staff turnover and responsibilities change and to supplement the technical and design resources of the Customer as required.



Senetas Corporation Limited ABN 33 006 067 607

Head office: Level 1, 11 Queens Road, Melbourne Australia 3004

Phone: 1800 261 114 | +61 3 9868 4555 | Fax: + 61 3 9821 4899

Email: enquiries@senetas.com