

Case Study

Australian Government Department

Tivoli Security Solutions

The Customer

The Customer is a large Australian government department who has a presence in all Australian states, capital cities and in the capital cities of most countries. The Customer is responsible for one of the most important and strategic roles of the Australian Government.



The Challenge

Significant political and legislative changes have led to business process redefinition and IT restructuring requirements within the organisation. The Department's IT infrastructure was overhauled and re-architected to conform to a Service Oriented Architecture, Single-Sign On, and portal-like end user access model. Reuse of existing IT assets was crucial to the overall solution.

Security was an important part of the solution. Security considerations included authentication of end user's distributed over wide geographical areas including international locations; authorization of end user access to resources and execution of business functions, when privacy and confidentiality were key considerations; and auditing and reporting requirements.

As a part of the solution and to facilitate seamless end user experience, single sign-on to applications and the ability for end users to reset their own LAN passwords and unlock their LAN accounts were also important requirements.

The Solution

The Customer's requirements were realised in two parts:

1. Single Sign-On to corporate applications.
2. Resetting of forgotten LAN passwords and unlocking LAN accounts by the end user.

Senetas Consultants were involved in the implementation of the IBM Tivoli Enterprise Single Sign-On product. In particular the following components of the ESSO suite were used:

IBM Tivoli Access Manager for Enterprise Single Sign On (TAM for ESSO)

TAM for ESSO acts as a proxy on behalf of an end user to enable that user to sign on to configured applications, without the user having to enter their credential for the target application. TAM for ESSO maintains an association between a user's Active Directory (AD) network operating system credential, and the credentials for all applications that the user has access to, and which TAM for ESSO is configured for. TAM for ESSO recognises login screens and change passwords screens of Windows, Web, Mainframe and java based applications, intercepts such screens, and then injects the user's credentials into the application. In this way, a user who signs-on to a corporate desktop is able to sign into all their applications, i.e. without having to enter their application



credential. Moreover, the application credentials are stored securely in a central location, thereby enabling single sign on when users move between desktops.

Desktop Password Reset Service

The Desktop Password Reset Service (DPRS) enables a user to reset their Active Directory password, if they have forgotten their password, or unlock their Active Directory account, if the user has been locked out of the Windows Domain. The end user is presented with a set of challenge questions, which the DPRS administrator has configured, and which the user has previously answered during an enrolment process. Upon answering the questions, the DPRS system computes a



Case Study

Australian Government Department

Tivoli Security Solutions

score based on the answers provided. If the score is above a predefined threshold, DPRS allows the user to reset their AD password or unlock their account. The user may then log onto their desktop.

Services Delivered

Senetas provided consulting resources for the implementation of the system, including ESSO and the DPRS. This included deployment and configuration of software components, problem identification and resolution and the documentation of implementation plans and system management plans.

The services provided during the project were:

- Review and update of Solution Design
- Solution implementation plan
- System management plan
- Solution Build – in conjunction with the Customer's staff
- Testing of Solution – in conjunction with Customer's staff, test the solution against the test plan to ensure requirements are met

The Benefits

The Customer's end users have experienced ease of use, as a consequence of being seamlessly signed onto applications, without having to enter application credentials, resulting in productivity increases. Active Directory password resets and unlocking of accounts are done by the end users themselves. This has resulted in a significant reduction in helpdesk calls and a commensurate reduction in help desk costs.

The Future

Senetas has continued to provide training to the Department's staff to help the Department to effectively manage their security infrastructure.

