

## CUSTOMER SUCCESS STORY – NESS TECHNOLOGIES



*“The inability to achieve compliance can bring enterprise operations to a halt. Global enterprises, such as ours, which handle project sensitive and confidential information, are mandated to stay compliant ensuring that we have best practices in place to secure information access. IMAG’s effective and innovative password management solution has enabled Apere to significantly reduce operating costs and enable us to meet regulatory requirements including BS-7799”.*

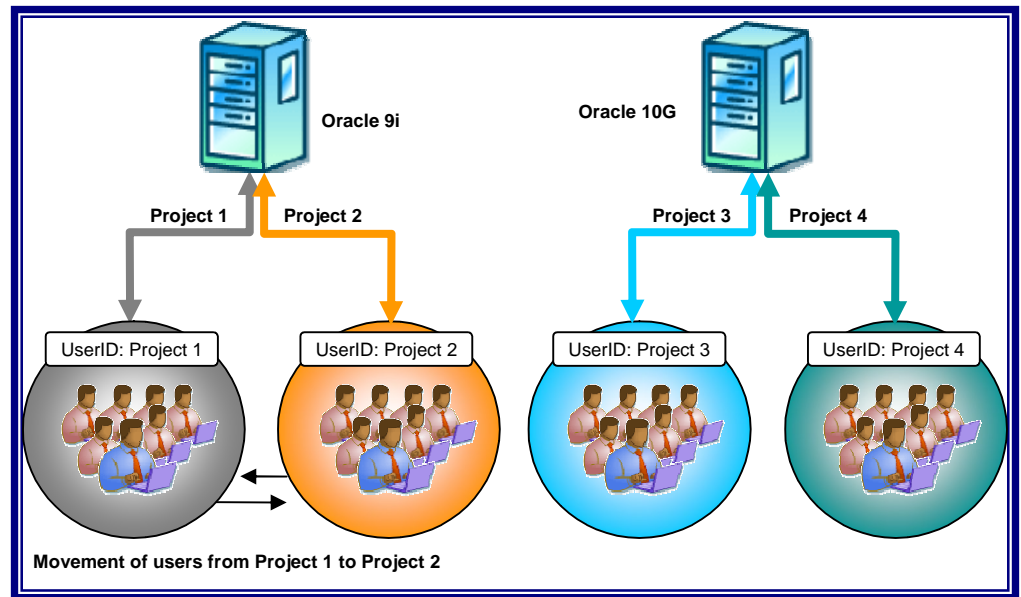
**Director IT,  
Ness Technologies**

### ABOUT NESS TECHNOLOGIES

Ness Technologies (NASDAQ: NSTC) is a global provider of end-to-end IT services and solutions designed to help clients improve competitiveness and efficiency. Ness specializes in outsourcing, offshore, systems integration, application development, consulting, quality assurance and training. With 7,500 employees, Ness maintains operations in 16 countries and partners with numerous software and hardware vendors worldwide.

### THE CHALLENGE: SHARED USER ACCOUNTS

To ensure customer satisfaction, Ness Technologies assigns 10 to 15 engineers to work on a single project, and a single application is assigned to two or more different projects. For example, Oracle 9i is accessed by teams working on Project I, Project II and Project III. For every project, only one User ID is created with an assigned project name. Every user who works on this project uses the same UserID, resulting in shared accounts. If one of the employees migrates or quits from the current assigned project he/she continues to have access to that shared account, resulting in a compliance violation and a serious security threat. Ness Technologies needed a process in place to manage these configurations.



Every user who works on this project uses the same UserID, resulting in shared accounts. If one of the employees migrates or quits from the current assigned project he/she continues to have access to that shared account, resulting in a compliance violation and a serious security threat. Ness Technologies needed a process in place to manage these configurations.

### THE SOLUTION – IMAG BY APERE

#### Managing Shared Accounts, Documenting Account Modifications and Securing Access

Prior to deploying IMAG, Ness was mapping each employee ID to a Project ID and then reconciling manually. As a result, every user who accessed an application under Project I was identified by a single User ID or Project ID, posing a serious security threat. However, with IMAG, when a user leaves a project he is un-reconciled from the shared-account. IMAG’s password management solution resets the password for the shared-account and sends an email notification to those users still on the Project, thus denying access by the un-reconciled user to the shared-account.

If due to absence or unavailability an email notification to delete an account is missed by an administrator, IMAG enables the project lead to instantaneously handle the situation, thereby eliminating any security exposure. IMAG also eliminates any potential loss of productivity which can be caused by inaccurate provisioning, because all provisioning activity is documented for review by Ness and its customer and can be used for compliance reporting.

#### Centralizing User Account Creation, Deletion and Disablement

A lack of centralized user account creation, deletion, and disablement forced Ness Technologies to implement an elaborate manual process whenever the company needed to make changes to user access or establish a new user account. Creating or deleting an account could take as much as 7 business days depending upon availability of the appropriate administrator and the steps required to establish a new user account across multiple applications. Steps typically required for creating an account include:

- Identifying the applications that the user needs to access

- Securing all required approvals and documenting the approvals
- Notifying the appropriate administrator to create the accounts
- Logging into and accessing each application individually
- Identifying the user ID and performing user ID related tasks
- Notifying the user and documenting the process, upon completion of the task

In a dynamic organization such as Ness Technologies, to ensure optimum business operations and productivity, the company needed to institute a more efficient process for modifying or deleting user access, as well as setting up new user accounts.

### Efficiently Tracking and Reporting User Account Activity across Multiple Projects and Networks

To address this issue, Ness Technologies deployed IMAG to centralize the identity management process, which reduced the process from days to minutes. And by centralizing this function, Ness was guaranteed that the creation of new user access was complete and fail-safe, without adding any administrative burden. In addition, when an employee account needs to be provisioned, Ness is assured that all of their rights, across applications and projects, have been purged, therefore meeting security and regulatory compliance requirements.

Equally important to tracking user account activity, is a reports repository and notification of reports to respective application authorizers. Accurate and complete reporting enables Ness Technologies to prove security or regulatory compliance, but to view those reports via a single point location was yet another challenge to the company, proving to be a time consuming activity.

With IMAG, Ness now has the ability to generate reports at a centralized location and send an email to the recipient with complete reporting data on a daily, weekly or monthly basis. These reports, which provide a quick glance at the health of their identity based security, can be stored and viewed by Ness management or the appropriate administrator via a simple, consolidated view into the identity access information to validate security posture and compliance with required regulations.

### The Results

IMAG enhanced the ease of managing shared user accounts across multiple applications and networks for Ness, while improving security for regulatory compliance, and maximizing administrative and user productivity.

In addition to ensuring complete accuracy, IMAG cut the process for creating or changing user accounts from days to minutes, significantly reducing administrative burden, while delivering a simple, consolidated view into the identity access information to validate security posture and compliance with required regulations.

### ABOUT APERE

Headquartered in San Jose, California, Apere was established by a group of experienced techno-entrepreneurs, and has been engaged in creating world-class products dedicated to offering state-of-the-art and yet cost-effective enterprise security solutions. Apere offers the industry's first Identity Managed Access Gateway designed to address identity and data security issues while significantly reducing the management burden placed on IT staff.

#### Ness Technologies Challenges

- Ensure best practices to achieve and maintain required regulatory compliance
- Eliminate potential security threats posed by unauthorized user access
- Implement an automated, efficient process for modifying or deleting user access, as well as setting up new user accounts
- Efficiently track and report user account activity across multiple projects and networks

#### Apere IMAG Solution

- IMAG significantly simplified the management of shared user accounts across multiple applications and networks
- IMAG improved security for regulatory compliance, and maximized administrative and user productivity
- IMAG ensured complete accuracy, and reduced the process for creating or changing user accounts from days to minutes, significantly reducing administrative burden

---

#### US Headquarters

2635 North First St Suite 212  
San Jose, CA 95134  
Phone: +1-408-434-1001  
Fax: 1-408.434.1002  
E-mail: [contact@apere.com](mailto:contact@apere.com)

#### India Research and Development Office

Apere India Pvt Ltd  
Plot # 14, Huda Colony  
Road # 02, Banjara Hills  
Hyderabad - 500 033  
Phone: +91-40-44308080  
Fax: +91-40-44308