

# AmTrust Reduced Database and Linux Helpdesk Calls by 80% with Centralized User Management

## AMTRUST BANK

AmTrust Bank  
Cleveland, OH  
www.amtrust.com

**Industry:**  
Financial Services

**Annual Revenue:**  
\$17 Billion, September 2007

**Employees:**  
2700

### Oracle Products & Services:

Oracle Database  
Oracle Internet Directory  
Oracle Application Server  
Oracle Business Intelligence EE  
Oracle Financial Analyzer  
Oracle Discoverer

### Key Benefits:

- 88% decrease of DB password related helpdesk calls
- 82% decrease of Linux password related helpdesk calls
- Improved user experience using a single password
- Efficient (de)provisioning of database and Linux users from Active Directory
- Highly available flexible authentication system

*" Oracle Internet Directory provides us a reliable and secure platform to easily centralize account management for Oracle databases, Unix/Linux systems, and business applications. The projects delivered high ROI. " – KP Singh, Database Administration Manager, AmTrust Bank*

AmTrust Bank was founded in 1889, and is one of the fastest growing financial institutions in America. AmTrust has grown from a local savings and loan with one office to a nationally recognized leader in retail banking, with branch offices in Florida, Ohio and Arizona.

As more applications and databases were deployed and more users were provisioned to support growing business, challenge of managing users consistently across applications, databases, and operating systems was ever increasing. Managing users in individual systems resulted in poor user experience due to multiple passwords, high administration cost due to redundant administration, and poor compliance due to inconsistent security policies and ineffective provisioning process.

To address these challenges, AmTrust Bank implemented Oracle Internet Directory (OID) centralizing database user management as well as Linux/Unix authentication. As a result, monthly helpdesk calls were reduced by an average of 88% for the DBA team, and by 82% for Unix administrators. In addition, OID integration with Active Directory (AD) streamlined the provisioning process and greatly improved end user experience as the same Windows credential is used to access databases, Linux/Unix, and applications.

### Centralizing Database and Unix/Linux User Management with Oracle Internet Directory

As AmTrust Bank decided to centralize the management of Oracle Database users and Unix/Linux accounts, requirements were well defined to ensure project success. In addition to high availability, the solution should not require any changes to existing applications, should not introduce any new security

procedures for end users, and should be able to leverage existing enterprise Active Directory to automate the process.

Based on the requirements, AmTrust Bank selected Oracle Internet Directory (OID).

Oracle Database provides a function called Enterprise User Security (EUS) to centralize user and role management using Oracle Directory Services, either OID or Oracle Virtual Directory (OVD). With EUS, instead of maintaining user information, and mapping DB roles and privileges to individual users in hundreds of DB's, the information is managed centrally in OID.

Since Microsoft Active Directory (AD) is the "source of truth" for identities within AmTrust Bank, it is critical for OID to integrate with AD to automate the entire user provisioning and de-provisioning process. Users and groups are directly managed in AD and then synchronized to OID. Although OID provides bi-directional data synchronization with Active Directory, at AmTrust Bank, only data synchronization from AD to OID is used to maintain AD's status as source of truth.

For the EUS deployment, OID users and groups are mapped to Enterprise users and Enterprise Roles in OID, which are then mapped to database schemas and database roles for authentication and authorization.

It is not uncommon that in large database deployments ineffective de-provisioning of DB users can lead to orphaned accounts. AmTrust addressed this potential compliance risk by leveraging EUS with OID where the user only needs to be disabled in OID or AD to prevent further access to any database.

Since Microsoft uses a proprietary way to hash passwords in Active Directory that is incompatible with the Oracle DB requirements, the password filter must be installed on the domain controller to capture password changes in order to hash and store them in a format required by the database. The password filter will be notified when a password change occurs, hashes the password in a DB compatible format, and stores the hash in AD. The password filter uses published Microsoft APIs to capture password change notification.

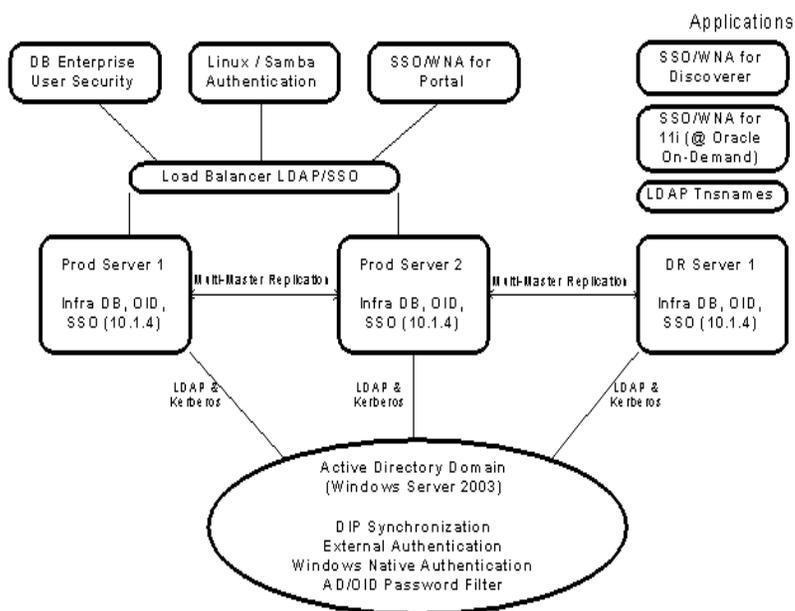
The implementation of the password filter enables users to use Windows credentials to log into databases and ensures a consistent password policy across databases and Windows.

The same OID infrastructure is used to provide a unified login experience for Linux/Unix users by centralizing Linux/Unix authentication using OID (the integration is made even easier with the recently released Oracle Authentication Services for Operating Systems product as integration and migration are automated). OID further enables the centralized management of Linux/Unix “sudo” access policies.

In addition, Oracle SSO server that provides single sign-on capability for Oracle Portal, Oracle Financial Analyzer and Oracle Discover also leverages the same OID infrastructure.

Implementing a centralized authentication requires high availability (HA). OID provides multiple layers of HA. Multi-master replication can be combined with database HA features like Oracle Real Application Cluster (RAC) and Oracle Data Guard for maximum availability architecture. AmTrust deployment leverages OID HA architecture to ensure system availability.

The following graphic gives an architectural overview of the AmTrust deployment.



### Why Oracle?

Simplifying Oracle database user administration was the initial driver for AmTrust, and OID was the default directory for Enterprise User Security deployment. “OID’s high scalability, availability, and security makes it a good fit for a critical component of the enterprise architecture that can be leveraged by many applications and systems.” Said, K.P., “In addition, the expertise and support offered from Oracle made AmTrust very comfortable to go for an Oracle solution.”