

ORACLE XELLERATE IDENTITY PROVISIONING

KEY FEATURES AND BENEFITS

ORACLE XELLERATE IDENTITY PROVISIONING

- **Increased security:** Enforce internal security policies and eliminate potential security threats from rogue, expired and unauthorized accounts and privileges
- **Enhanced regulatory compliance:** Cost-effectively enforce and attest to regulatory requirements (e.g. Sarbanes-Oxley, 21 CFR Part 11, Gramm-Leach-Bliley, HIPAA) associated with identifying who has access privileges to sensitive data
- **Streamlined operations:** Reduce inefficiency and improve service levels by automating repeatable user administration tasks
- **Improved business responsiveness:** Get users productive faster through immediate access to key applications and systems
- **Reduced costs:** Reduce IT costs through efficient staff usage and common security infrastructure.

Oracle Xellerate Identity Provisioning is a powerful and flexible enterprise identity management system that automatically controls user accounts and access privileges within enterprise IT resources. Part of Oracle Identity Management, it provides user management for the entire identity lifecycle – from the initial creation of accounts to their termination – all the while adapting to the changing business requirements of the enterprise. Oracle Xellerate Identity Provisioning and Oracle Identity Management are components of Oracle Fusion Middleware.

Introduction

Oracle Xellerate Identity Provisioning is a robust enterprise provisioning solution built on a J2EE-based, N-tier deployment architecture that separates the platform's presentation, business logic and data tiers. This separation of tiers enables Xellerate to rapidly scale with the performance needs of the deployment. The architecture is also able to leverage the most flexible and supported cross-platform J2EE services available such as Java, XML, and object technologies.

Workflow and Policy Management

Xellerate's workflow and policy management capabilities enable policy-based, automated provisioning of resources and fine-grained management of entitlements within resources. It provides an easy way to build provisioning workflows, the business processes that govern the steps by which provisioning transactions are executed, which are then implemented with the Xellerate logic.

Identity Reconciliation

One of Xellerate's most powerful features is its Identity Reconciliation Engine, which allows it to police resources under its management. If Xellerate detects any accounts or changes to user access privileges effected outside of its control, it can immediately undo the change or notify an administrator, depending on how it is configured at deployment. This allows easy detection of rogue and orphan accounts and is indispensable for meeting compliance requirements.

Reporting and Auditing

Xellerate also provides comprehensive reporting and auditing of the application environment, allowing automated collection of information about users (including their current and historical access privileges) and resources (such as who has access to them now or in the past) to support compliance with regulations such as Sarbanes-Oxley, 21 CFR Part 11, Gramm-Leach-Bliley and HIPAA.

ORACLE IDENTITY MANAGEMENT PRODUCTS

Oracle Identity

Management is an integrated, scalable and robust identity management infrastructure that includes LDAP V3 directory services, directory synchronization, access management and a certificate authority.

Oracle COREid Access

and Identity delivers critical functionality for access control, single sign-on, and user profile management in the heterogeneous application environment.

Oracle COREid Federation

enables cross-domain single sign-on with the industry's only identity federation server that is completely self-contained and ready to run out-of-the box.

Oracle Xellerate Identity

Provisioning is a powerful and flexible enterprise identity management system that automates the creation, updating, and removal of users from enterprise systems such as directories, email, databases, and ERP.

Oracle Web Services

Manager is a comprehensive solution for adding policy-driven security and management capabilities to existing or new Web services.

Oracle Virtual Directory

provides Internet and industry standard LDAP and XML views of existing enterprise identity information, without synchronizing or moving data from its native locations.

Self-Service Management

Xellerate's self-service management, delivered through the Xellerate Web Administration Console (Figure 1), allows end-users to view, manage and update their own profile data, including passwords, across managed resources. If a user has forgotten his password, Xellerate presents customizable challenge questions to enable identity verification. Users can also create requests for accounts and privileges. Business approvers can then use the same interface to examine and approve incoming requests.

Delegated Administration

With Xellerate, administrators can delegate administration functions such as account creation and request approvals to groups, organizations and individuals, making it possible to efficiently manage large populations of users across many resources.

Adapter Factory®

Xellerate's Adapter Factory® facilitates rapid integration to commercial or custom systems without programming. Once adapters have been created, their definitions are maintained within the Xellerate repository, creating self-documenting views. These views make extending, maintaining and upgrading connections a manageable and straightforward process. Oracle Xellerate Identity Provisioning also includes a library of pre-configured adapters that support many common resources, each of which can be reconfigured or extended via the Adapter Factory.

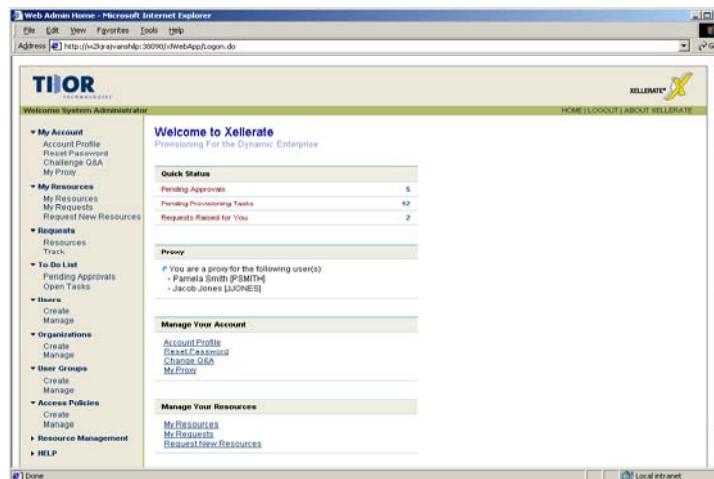


Figure 1. Xellerate Web Administration Console

Conclusion

Oracle Xellerate Identity Provisioning is the industry's best solution for managing accounts and privileges for enterprise application users. A component of Oracle Identity Management, Xellerate is part of Oracle's complete enterprise solution for identity management and application security.