Integrated Account Management and Access Control System

Omni-IM

Enhanced Convenience and Security of the Server Management!
Effective Process of the Automated Account and Privilege Management!!

Omni-IM is the approval-based integrated account management and access control system that manages user accounts of heterogeneous OSs and DBMSs through the Omniguard solutions, as well as the life cycle and access authority from account creation to destruction.

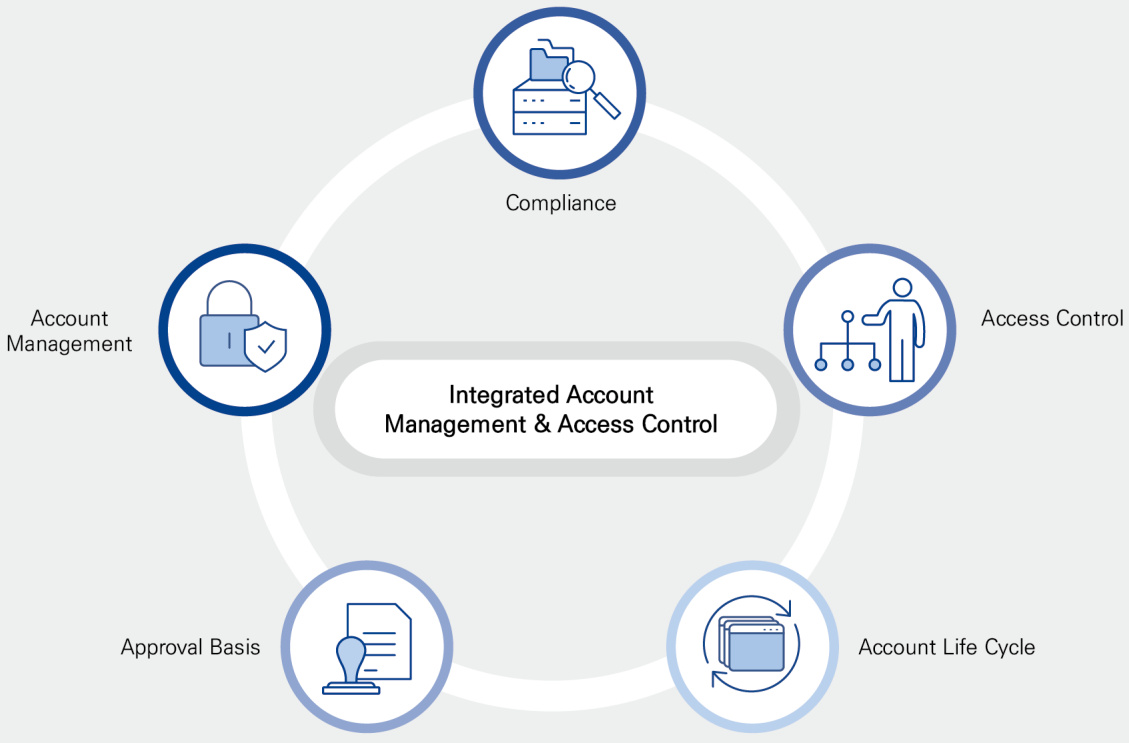
Overview

The Need for Efficient Integrated Management Server Security

- Increase in the value of personal information handled and various information systems
- Concerns about excessive cost burden when managing the system account management and controlling the access
- Growing issues on the tightened regulatory and legal requirements and responses
- Rise of threats by internal users

The Need for Automated Account and Access Authority Management Suitable for Workflow

- Increased difficulty in automating and centralizing account lifecycle management
- Threats to unmanaged accounts
- Growing intrusion attacks through various routes
- Changes in the user account information and access authority, such as retiring the company or transferring to a department



LSware Inc. 18th floor, Daeseong D-polis Building A, 606, Seobusaet-gil, Geumcheon-gu, Seoul, Republic of Korea, 08504
TEL +82-2-6919-0321 FAX +82-2-6919-0329

Key Features of Omni-IM

Provision of Account Mgmt. Process

- Account life cycle management (Providing Workflow)
- Interworking with internal systems such as HR/SSO/ mail systems
- Automatically reflected and synchronized to the pertinent system according to the account application/approval process

Access Control

- Providing approval processes such as a request for approval on access
- Setting system access authority for each account
- Supporting access control to OS/DBMS
- Changing authority in conjunction with HR information when the status of personnel is changed

Account Management

- Automated account checking (detecting Ghost accounts)
- Viewing and changing the information on the user-owned/managed accounts
- Actions and alarms for various account status such as a change in HR /non-registration/unauthorized change
- Providing the feature to manage the domain, personnel in charge of server and retirement

Report

- Statistics on the account status and workflow status
- Providing a screen suitable for the user authority and management scope
- Providing the features to create and download various reports
- By detecting the status of the account, the system automatically sends an email to the account holder, the person in charge of account management, and the head of the department.

Advantages of Omni-IM

Easy

- Easy to install without changing N/W and App according to the introduction
- Easy to apply and expand through the simple installation of the Agent and Manager
- Providing user portal to support the convenient approval process-based features

Convenient

- No change from the user's point of view as the existing login method is used as it is
- Easy maintenance because there is no reboot or environment setting change when installing/removing Agent
- Simple configuration and easy to apply/remove for each security function

Safety

- Architecture configuration that minimizes impact on business systems
- Certain loads and anomalies do not affect the overall service
- There is no risk of changing existing applications and settings

Guide

- Extensive inspection on/checking for items that tamper with account attributes
- Applying no-exception security features for bypass and local users
- Easy to purchase selectively and apply the various security functions

Mapping for Core Elements, Laws, and Guidelines

Core Elements	Key Certification Guidelines
Information Security Management System (ISMS)	• Including control items in Article 19-10 (Access Control), such as limiting the number of failed logins/access user authentication/password complexity in items such as user authentication, password management, user registration, and authorization
Personal Information Security Management System (PIMS)	• Article 8 (Technical Protection Measures) In consideration of legal requirements and external threat factors, the password management procedures for personal information handlers, users, and information principals (users) shall be established and implemented. Accounts and authorities (privileges) granted to the personal information and personal information processing systems for special purposes shall be identified and separately controlled.
Regulation on Supervision of Electronic Financial Transactions	• Article 32 (Management of Passwords of Internal Users) A finance company or electronic financial business entity shall reflect the following matters in the information processing system in order to prevent the leakage of the passwords of internal users. • Article 13 (Computational Data Protection Measures) User accounts and passwords shall be assigned to each individual, and their registration, change, and deletion shall be systematically managed.
Technical and Administrative Personal Information Safeguard and Security Standard	• Article 4 (Access Control) Information and communications service providers, etc. shall establish rules for creating passwords including the following matters for personal information handlers, and apply and operate them (They must be composed of at least 10 digits or more by combining at least two types among the English letters, numbers, and special characters, or at least 8 digits by combining at least 3 types of those, etc.).

※ Relevant laws and regulations

Ministry of Science and ICT(Former Ministry of Science, ICT and Future Planning)"Notification on Personal Information Security Management System Certification, etc."
Korea Communications Commission "Notification on Personal Information Security Management System Certification, etc.", "Technical and Administrative Personal Information Safeguard and Security Standard"
Financial Services Commission "Regulation on Supervision of Electronic Financial Transactions"