SmartCloud®

NTT COMWARE

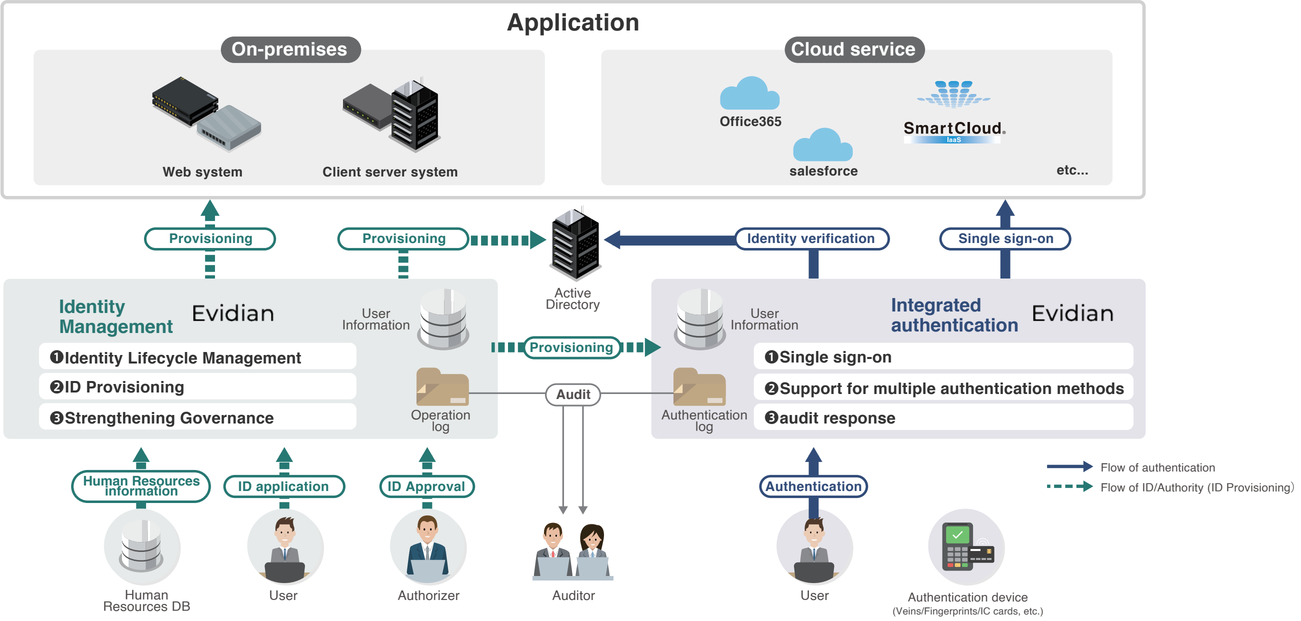
IAM Solution

Improve security and governance with proper identity management
Integrated application-specific authentication for single sign-on

※IAM：Identity & Access Management

Service Overview

- Identity Management：Centralized management of authentication and authorization information through a company-wide platform. In addition, by centrally controlling workflows such as ID submission and approval, we properly manage the ID lifecycle and strongly support governance, including auditing.
- Integrated authentication：Hybrid single sign-on (SSO) to on-premises systems and public clouds by building an integrated foundation for authentication of multiple applications.



Application

On-premises

Web system

Client server system

Cloud service

Office365

salesforce

SmartCloud® IaaS

etc...

Provisioning

Provisioning

Active Directory

Identity verification

Single sign-on

Identity Management Evidian

User Information

❶Identity Lifecycle Management

❷ID Provisioning

❸Strengthening Governance

Operation log

Provisioning

Audit

User Information

Integrated authentication Evidian

❶Single sign-on

❷Support for multiple authentication methods

❸audit response

Authentication log

Human Resources information

ID application

ID Approval

Authentication

Human Resources DB

User

Authorizer

Auditor

User

Authentication device (Veins/Fingerprints/IC cards, etc.)

Flow of authentication

Flow of ID/Authority (ID Provisioning)

Identity Management

Feature 1 Identity Lifecycle Management

- Define the ID lifecycle submission and approval process as a workflow to manage responsibilities within the workflow.

Feature 2 ID provisioning

- In cooperation with the Human Resources DB, in addition to "ID", "Permissions (Role)" according to the organization and job title are automatically linked to the necessary application/AD/integrated authentication infrastructure.

Feature 3 Strengthening governance

- It is also possible to automatically grant access authority (segregation of duties) to the ID according to the organization to which the user belongs.
- Reconciliation (Identity management and identity/access authority matching between AD/applications) can be done manually or automatically, and if differences are extracted, they can be corrected immediately.
- Manage logs of who has access to what applications, when, who created, modified, and deleted what identities for efficient audit response.

Integrated authentication

Feature 1 Single sign-on

- It offers hybrid SSO capabilities across both on-premise and public clouds to enable single sign-on regardless of the application environment you want to use.
- Single sign-on eliminates the need to establish authentication policies such as password assignment rules for individual applications.
- You can reduce licensing costs by arranging products to be deployed according to the type of application you want to use (Web/client-server/public cloud).

Feature 2 Support for multiple authentication methods

- It supports various authentication methods such as IC card/PIN code/one-time password/fingerprint/biometric authentication using a vein, and provides an authentication mechanism that meets security requirements.

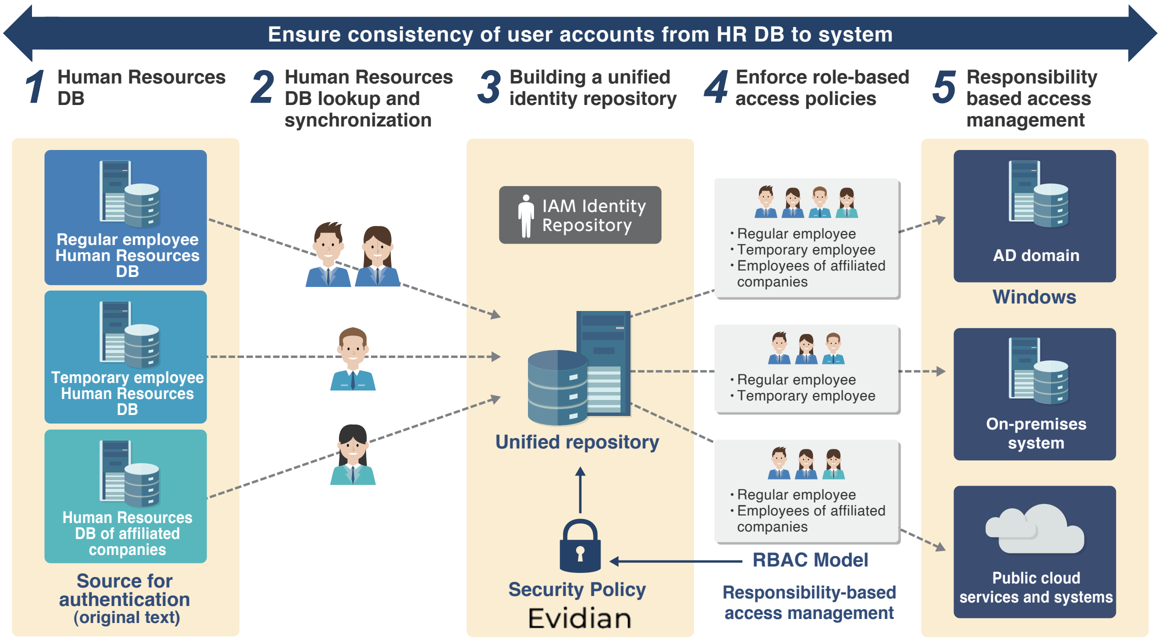
Feature 3 Audit response

- Log who logged in, when, and to which applications for efficient audit response.

Usage Image

Ensure consistency of user accounts from HR DB to system

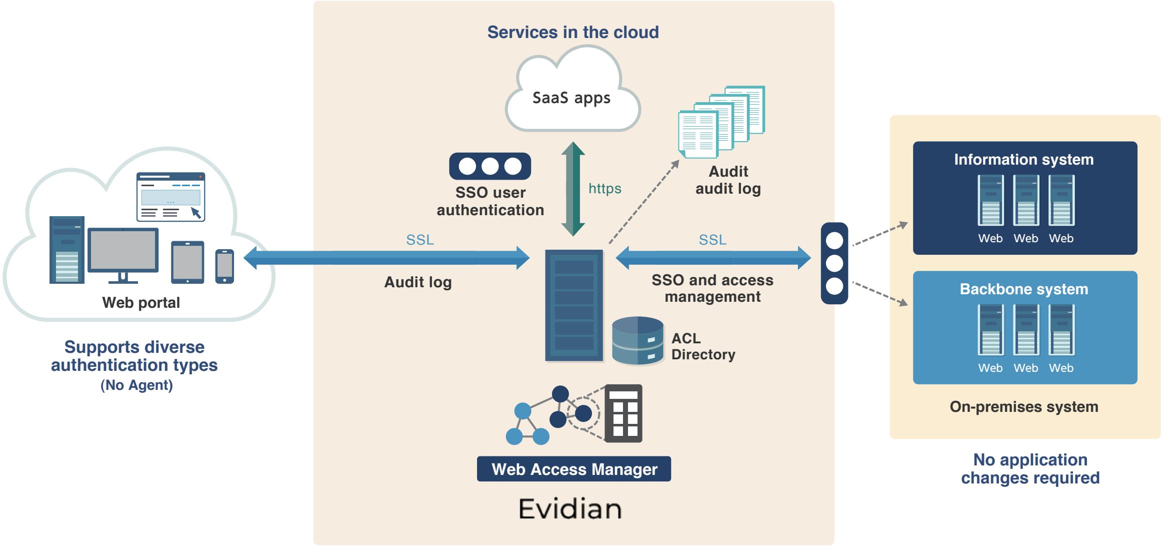
An integrated identity repository that synchronizes with various human resources databases applies responsibility-based access policies to accurately update user account information for various systems and services on premises and in the public cloud.



Ensure consistency of user accounts from HR DB to system
1 Human Resources DB
2 Human Resources DB lookup and synchronization
3 Building a unified identity repository
4 Enforce role-based access policies
5 Responsibility based access management
Regular employee Human Resources DB
Temporary employee Human Resources DB
Human Resources DB of affiliated companies
Source for authentication (original text)
IAM Identity Repository
Unified repository
Security Policy
Evidian
・Regular employee
・Temporary employee
・Employees of affiliated companies
・Regular employee
・Temporary employee
・Regular employee
・Employees of affiliated companies
RBAC Model
Responsibility-based access management
AD domain
Windows
On-premises system
Public cloud services and systems

Single sign-on via web portal, enhanced control over access to web applications

Enables single sign-on with agentless support for a variety of authentication methods from a variety of terminal web portals, enabling integrated access management to public cloud, on-premise services, and systems without application changes.



∗Evidian is a registered trademark of Eviden.

∗The contents of the products and services are subject to change without notice.
∗"SmartCloud (Smart Cloud)"and the "SmartCloud" logo are registered trademarks of NTT COMWARE CORPORATION in Japan.
∗Active directory and Office365 are registered trademarks of Microsoft, its subsidiaries and affiliates in the United States and other countries.
∗Other company names and product names may be trademarks or registered trademarks of their respective companies.

NTT COMWARE CORPORATION
1-9-1 Kounan,Minato-ku, Tokyo 108-8019 Japan
https://www.nttcom.co.jp/english/

2023.11
V5.2.0