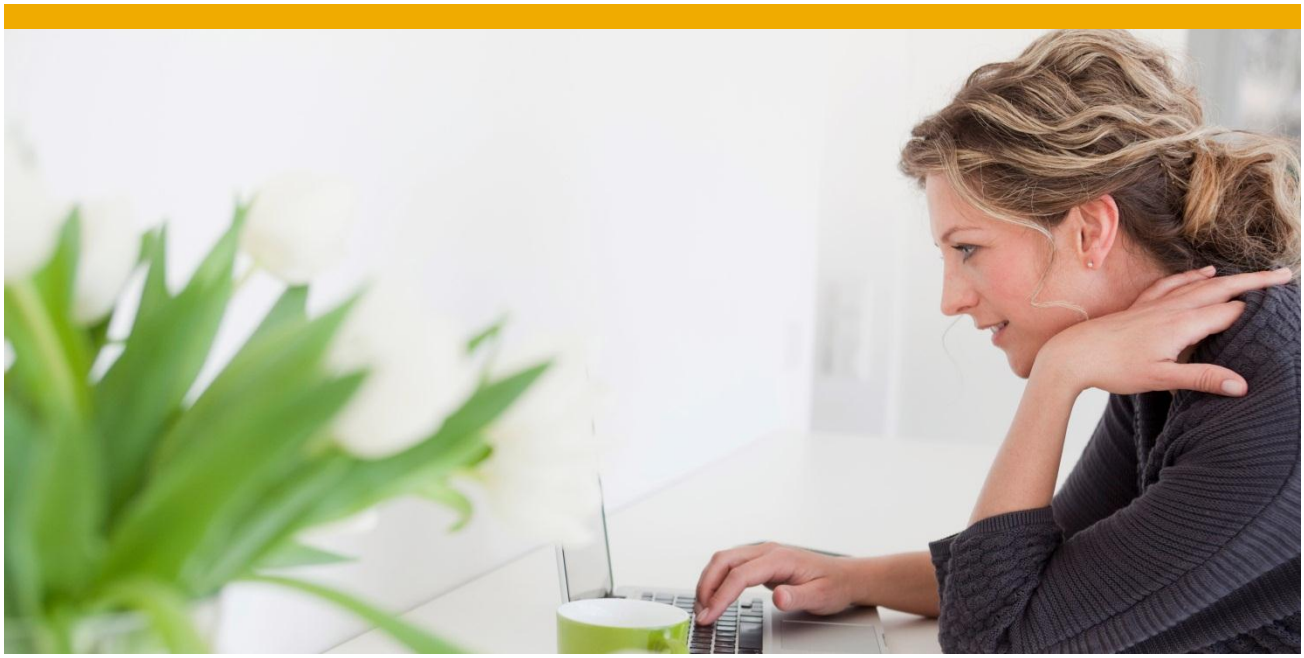


How to Leverage SAP NetWeaver Identity Management and SAP Access Control Combined Solutions

TABLE OF CONTENTS

INTRODUCTION **3**
SAP Netweaver Identity Management **4**
SAP Access Control **4**
COMPARISON OF MAJOR PRODUCT FEATURES **5**
Deployment Considerations **6**
Case Study **9**
SUMMARY **10**
AUTHOR SUMMARY **10**

INTRODUCTION

This paper provides an overview of the integrated solution and a summary of implementation options for deploying a combined solution based on SAP Access Control and NetWeaver Identity Management. This solution combines access governance and identity management capabilities to support automation of identity and access processes and compliance requirements.

- SAP Access Control solution is based on ABAP technology and integrates with the native SAP ERP, Oracle, PeopleSoft, and JDE interfaces to support access governance capabilities. These capabilities include features such as administration of the access request process and approval process with integrated SOD analysis.
- NetWeaver Identity Management is based on Java technology and is designed to support administration of user identities, user provisioning, and single sign-on across IT systems and applications.

SAP Access Control provides highly specialized functionality required to administer access and manage accounts to meet requirements for financial regulations and company policies. NetWeaver Identity Management provides powerful features designed to automate identity administration across multiple systems. When IdM is integrated with SAP Access Control, SoD analysis capabilities can be integrated with the approval processes within IdM to ensure that role assignments are compliant with financial regulations.

Please read on to learn more about the benefits of the integrated solution and how to best leverage the features of each to determine the best approach for your deployment

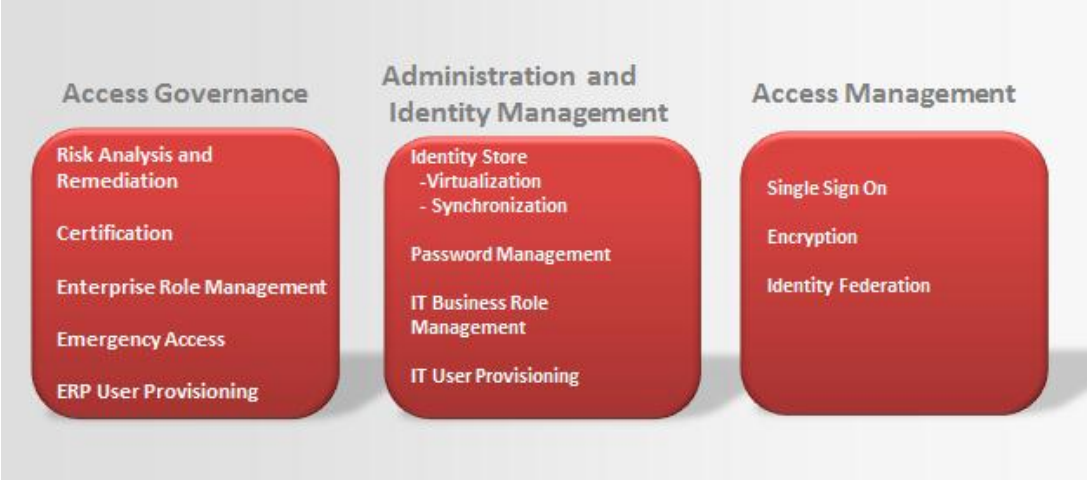


Figure 1. Features of NetWeaver Identity Management and SAP Access Control

SAP Netweaver Identity Management

SAP NetWeaver Identity Management (NW ID Mgmt) provides a comprehensive solution for managing user accounts and privileges across enterprise landscapes. Enterprise landscapes include a variety of applications and systems such as Microsoft Active Directory, Microsoft Exchange, SAP Business Suite, and custom applications. SAP NetWeaver Identity Management is capable of integrating with these systems to support identity management and provisioning through a combination of out-of-the-box connectors, standards-based integration, connectors provided by partners and connectors custom-developed using the NW ID Mgmt's published connector API.

NW ID Mgmt supports the functionality to manage the user lifecycle from initial on-boarding, change, and termination. NW ID Mgmt includes an integrated workflow engine, extended Role-Based Access Control, and an integrated Identity Store built on virtual directory technology, the authoritative source for user identity data. NW ID Mgmt provides password synchronization functionality, allowing users to change their passwords on a number of source systems and have those passwords synchronized across all of their different accounts. Comprehensive reporting of activities relating to the mappings of users, roles and privileges are provided through SAP Business Warehouse.

Standards-based Web Single Sign-On functionality is provided through a SAML 2.0 compliant Identity Provider. In addition, the product includes a Virtual Directory component that provides valuable meta-directory functionality and forms the engine for the product's connector API.

SAP Access Control

SAP Access Control is an access governance solution that automates the processes associated with managing access to business applications. SAP Access Control supports processes and audit records that track who has access, who approved access, when access was granted, and if the access assignments are still required.

SAP Access Control is designed to bridge the gap between obtaining the technical definitions of system authorizations and facilitating the process of associating the correct system authorization or entitlement with the appropriate user. SAP Access Control includes the following five modules to accomplish this automation

- Access Request Process – integrated workflow process to orchestrate approvals, SoD analysis, account actions (ie create, delete, lock, unlock, etc), and automated role assignment
- User, Role, and Risk Certification – supports a periodic review process for existing user assignments, role definitions, and access risks required by several compliance regulations
- Risk Analysis and Remediation – enables analysis of Segregation-of-Duty (SoD) violations by role, business process through ad-hoc queries or integrated with the access request. The integrated risk analysis enables stakeholders to resolve conflicts and reduce risk by mitigating the violation by changing the role assignment or through a mitigating control.
- Business Role Management – supports management of SAP technical and business role lifecycle management. SAP Business Role Management enables the centralized management of SAP technical roles across multiple systems using a role methodology. This process ensures that roles are subjected to appropriate testing and approvals prior to deployment. Business roles in SAP BRM are groups of entitlements that can be associated with job functions for easily assignment to business users.
- Emergency Access Management – a complete solution for managing access for privileged user access with integrated monitoring and log review.

SAP Access Control is built on SAP ABAP technology and is supported using standard SAP basis and transport processes. SAP Access Control is intentionally built as a stand-alone solution to support integrated compliance and access provisioning for SAP ERP systems.

COMPARISON OF MAJOR PRODUCT FEATURES

This section compares key features of NetWeaver Identity Management and SAP Access Control.

FUNCTIONALITY	NETWEAVER IDM Identity Administration and Provisioning	SAP ACCESS CONTROL Access Governance and ERP Provisioning
User Provisioning	User provisioning based on Java technology, connector framework, and integrated Identity Store for systems and applications. Broad support for SAP applications, databases, LDAP Directories, replacement for SAP CUA.	Supports access request, approval processes, default values, role mapping, HR position based security, account actions and specific features required for managing access for ERP systems; based on SAP ABAP technology.
Role Management	Job function oriented, SAP and Non-SAP roles supported including global heterogeneous cross-system business roles. Supports context based grouping of roles and hierarchical role inheritance capabilities.	Includes SAP technical role lifecycle management, integrated risk analysis, business role management. Focus is on definition and support of SAP business processes.
Workflow	Comprehensive workflow designed for general IT on-boarding and off-boarding.	Specifically designed multi-stage multi-path to handle multiple line item requests, cancelation and forwarding scenarios for access request approvals, delegation, and certification processes required for financial integrity and compliance.
Access Certification	Customizable configuration in the product.	Complete solution for periodic analysis and certification of user assignments, role definitions and access risk. Supports process that enables review scope to be defined and administrative review process, and review management.
Segregation of Duties Analysis	Not Supported	Flexible and comprehensive cross-system SoD and Critical Action risk analysis
Reporting and Auditing	Designed for management of user provisioning processes	Supports compliance audit requirements
Single Sign-On	Standards based SSO for SAP	Not Supported

	and non-SAP applications based on SAML 2.0.	
Identity Provider	Standards based IDP for SAP and other third party applications and services	Not Supported
Emergency Access Management	Not Supported	Comprehensive application for emergency access management with integrated audit review process
Identity Store	Comprehensive support for virtual profiles and synchronization of identity profiles and attributes	User and role repository for compliance processes and reporting
Password Management	Comprehensive solution for password reset and policies	Supports reset only across multiple ERP systems
HR Integration	Automated update of user identities and synchronization with integrated systems	Automated ERP account provisioning based on HR event type and pre-configured default attributes and settings

Table 1. Feature Comparison

Deployment Considerations

Since both SAP Access Control and NetWeaver Identity Management were designed as independent solutions, there are several options to consider when integrating Access Control to an existing NW ID Mgmt deployment and vice versa. Along with these options, are important considerations for approval processes and management of the integrated solution.

Figure 2. Solution Architecture

For existing SAP Access Control customers, integration of NW ID Mgmt can enable common integrated workflow approval and provisioning process that includes IT, email, and business applications. Access requests can be initiated in the IdM system with subsequent approvals and analysis in Access Control. This solution helps to consolidate identity and access administration processes with automated workflow, provisioning, and integrated SoD analysis.

Existing Access Control Deployments
Considerations for Implementing an Integrated Approval Workflow – - Access request initiated in IdM, then send to Access Control to enable integrated approval process - Approval process supported in Access Control for all assignment provisioning actions. - Mitigating control concept in Access Control cannot be supported with external approvals. - Application roles are required to be maintained in Access Control and NW ID Mgmt to support risk analysis and approvals - User provisioning to ERP applications supported by Access Control - User provisioning to non ERP applications and IT systems can be supported using NW ID Mgmt Identity Store and connector framework. - Integrated audit trail supported through bi-directional web service – records all approval and request actions. - Access Control role management supports ERP role lifecycle - Emergency Access capabilities supported through SAP Access Control - Integrated reporting supported through BW

Table 2. Options for Existing SAP Access Control Customers

For existing NW ID Mgmt customers, you can benefit from integrating Access Control to support access governance and compliance features required to manage access to the ERP system. Access Control also includes role management, emergency access management, and reporting/ audit features that enhance and expand the value of NW ID Mgmt .

Existing NetWeaver Identity Management Deployments

Considerations for integrating Access Control access governance and compliance -
- Enables support for financial compliance and internal policies during provisioning approval process
- SoD Check web service enables check for conflicts during approval process
- Maintenance of roles is required in both SAP Access Control and NW ID Mgmt
- Access certification processes can support periodic reviews for all ERP and compliance relevant role assignments
- Multiple options for provisioning are supported:
  o Access Control supports ERP provisioning, NW ID Mgmt supports other systems and applications
  o NW ID Mgmt supports provisioning to all systems and applications
  o Access Control supports SAP HR Indirect position based security and provisioning model
- Maintains audit record of approval actions that enables
- Roles maintained with Access Control role management, enabled for NW ID Mgmt provisioning
- Emergency Access capabilities supported through SAP Access Control
- Integrated reporting supported through BW

Table 3. Options for Existing NetWeaver Identity Management Customers

Case Study

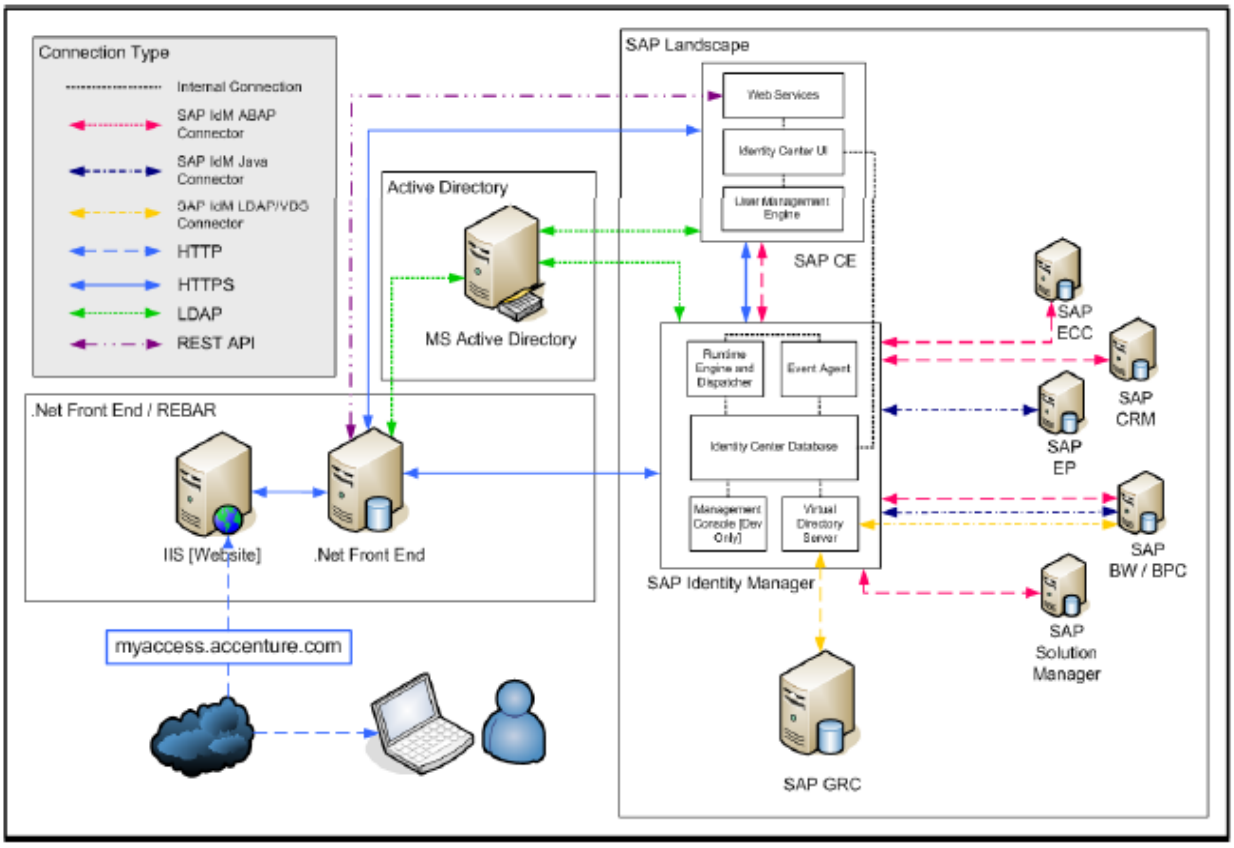
Company: Accenture

Quick Facts:
Revenue: USD $26 billion annually with Six working days to close accounting books
Countries: Over 120 Countries, 13 Geographic Unit, 3 Geographic Areas
Employees: Over 244,000

Objectives

- Achieve Access Risk as a part of the user provisioning process
- Reduce Access Risk and adverse compliance events across the enterprise
- Perform real time access risk analysis, alerts and reporting by integrating with NW Identity Management.

Integration scenario



In the above scenario, NW ID Mgmt is the leading system initiating a compliance check request to GRC Access Control. The Access Control application remediates any access risk associated to the users' request before handing it back to IdM to provision to SAP applications.

Benefits

- Reduced cost of operations by automating manual processes
- Gained a real time view of system compliance and ability to present this to auditors on demand
- Dramatically improved ability to respond to governance issues and potential violations

SUMMARY

Managing access to enterprise systems is becoming increasingly complex with increased risk and potential for penalties. Netweaver Identity Management and SAP Access Control combined solutions provide critically important features to ensure both management of identities and governance processes.

In many organizations, the management of IT systems and financial applications are supported by different organizations, however the processes are similar in some cases. The integrated solution of IdM and Access Control provides the ability to share a common set of tools to manage IT and ERP access and identity built on common workflow, roles, and processes enabling greater value for both NW ID Mgmt and Access Control customers.

AUTHOR SUMMARY

©Swetta Singh, Chris Radkowski, Keith Grayson
SAP Solution Management
December 6, 2012

www.sap.com