SAP Identity Management
Overview
SAP SE
June 2019
Agenda

Introduction to SAP Identity Management
Role Management and Workflows
Business-Driven Identity Management
Compliant Identity Management
Reporting
Password Management
Connectivity
Architecture
Identity Virtualization
Summary and Additional Information
Introduction to
SAP Identity Management
SAP Identity Management in SAP’s security products portfolio

**Security and threat intelligence:**
- SAP Enterprise Threat Detection
- SAP Identity Management
- SAP Cloud Platform Identity Provisioning
- SAP Single Sign-On
- SAP Cloud Platform Identity Authentication
- SAP NetWeaver AS, add-on for code vulnerability analysis
- SAP Fortify by Micro Focus (formerly SAP Fortify by HPE)

**GRC portfolio:**
- SAP Access Control
- SAP Cloud Identity Access Governance, access analysis service
- SAP Process Control
- SAP Audit Management
- SAP Business Integrity Screening (formerly SAP Fraud Management)
- SAP Risk Management
- SAP Identity Analytics
- SAP Business Partner Screening
- SAP Global Trade Services
- SAP Electronic Invoicing for Brazil (SAP Nota Fiscal Eletronica)

**GRC solution extensions:**
- SAP Access Violation Management by Greenlight
- SAP Regulation Management by Greenlight, cyber governance solution
- SAP Dynamic Authorization Management by NextLabs
- SAP Enterprise Digital Rights Management by NextLabs
What are the key capabilities?

Enables the efficient, secure, and compliant execution of business processes

Consistent user roles and privileges

SAP Identity Management

Holistic approach

Manage identities and permissions

Ensures that the right users have the right access to the right systems at the right time

Across all systems and applications
Business drivers for identity management

**Operational costs**
- Multiple sources of identity data
- Manual user provisioning
- Labor-intensive, paper-based approval systems
- Manual password reset processes

**Changing business processes**
- Transactions involve multiple enterprises
- Partners participate in business processes
- Company-specific requirements for user provisioning solutions

**Compliance challenges**
- No record of who has access to which IT resources
- Inability to deprovision user access rights upon termination
- No complete audit trail available
- Prevention of unauthorized access in multi-enterprise environments
Covering the entire identity lifecycle

- How long does it take for new employees to receive all permissions and become productive in their new job?
- Are permissions automatically adjusted if someone is promoted to a new position?
- How can you remove permissions automatically if employees change their position?
- Who has adequate permissions to fill in for a co-worker?
- How long does it take to remove ALL permissions of an employee? And how can you ensure that they were properly removed?
Solution in a nutshell

- Central management of identities throughout the system landscape
- Rule-driven workflow and approval process
- Extensive audit trail, logging, and reporting functionality
- Governance through centralized and auditable identity data
- Compliance through integration with SAP Access Control
- Compliant and integrated identity management solution to mitigate segregation-of-duties risks
Beyond compliance: Functional Components in a Business-driven identity management

- **Example: On-boarding**
- **Compliance checks**
- **Central identity store**
- **SAP Access Control**
- **SAP Identity Management**
- **Identity virtualization and identity as a service**
- **Provisioning to SAP and non-SAP systems**
- **Rule-based assignment of business roles**
- **Approval workflows**
- **Password management**
- **Integration with SAP Business Suite and SuccessFactors**

**Features**:
- **SAP ERP HCM**
- **SAP ERP HCM**
- **SAP BusinessObjects Access Control (GRC)**
- **SAP Identity Management**
- **SuccessFactors**
Solution in detail

Role management and workflows
How to define and provision roles

Role definition (design, one-time task)
- Read system access information (roles, groups, authorizations, etc.) from target systems
- Define a business role hierarchy
- Assign technical roles to business roles
- Develop rules for role assignments

Provisioning (regularly)
- Assign or remove roles to/from people
  - Through request/approval workflow
  - Manually (administrator)
  - Automatically, e.g. HR-driven
- Automatic adjustment of master data and assignments of technical authorizations in target systems
How to reduce complexity with context-based role management

Context-based role management simplifies the structure of roles through dynamic role assignment based on user context information.

Benefits
- Reduced number of roles
- Reduced complexity
- Sufficient granularity
- Improved data consistency and governance

Example:
20 roles in 1000 factories
- Conventional method: 20,000 entries (roles)
- Context-based: 1,020 entries (roles + contexts)
It’s up to you: Defining workflows

**Notification**
Identity Center sends a notification to user/manager

**Request**
User sends a role request

**Provisioning**
Identity Center provisions new roles and privileges to respective systems

**Processing**
Identity Center processes request
- Sends alert to manager/administrator

**Approval**
Manager checks request and approves/denies
Solution in detail

Business-driven identity management
Integration with SAP business applications

SAP Identity Management

- SAP Portfolio and Product Management
- SAP Customer Relationship Management
- SAP Supplier Relationship Management
- SAP Product Lifecycle Management
- SAP Service Parts Planning
- SuccessFactors Employee Central
- SAP Supply Network Collaboration
- SAP Extended Warehouse Management
- SAP ERP Financials
- SAP ERP Human Capital Management
- SAP Transportation Management
- SAP HANA
- SAP ERP Human Capital Management
- SAP Supplier Relationship Management
- SAP Customer Relationship Management
- SAP Portfolio and Product Management

© 2019 SAP SE or an SAP affiliate company. All rights reserved. ǀ PUBLIC
Kim Perkins joins the company as a marketing specialist. From the first day with her new company, she is able to log on to all relevant systems, including access to the employee self-services, and access to SAP CRM to track the marketing activities she is responsible for.

**1 Pre-hire phase**
HR ensures that all necessary employee data for Kim is available, such as position and entry date.

**2 Event-based extraction of personnel data**

**3 Based on the position in HCM, IDM automatically assigns the business role “Marketing Specialist”**

**4 Kim’s manager approves the assignment**

**5 First day at work**
Provisioning of role and authorization information to relevant target systems

- User created “Employee”
- Business Partner created “Marketing Professional”
- User created Access to SAP ESS
- Access to SAP CRM
After two years as a marketing specialist, Kim is promoted and takes over personnel and budget responsibility for her marketing team.

On the first day in her new role, she has access to the manager self-services. In her new position, she is responsible for budget approvals for all marketing campaigns – this requires immediate access to SAP ERP to view the marketing costs.

1. HR ensures that all necessary employee data for Kim is available.

2. Event-based extraction of personnel data

3. SAP Identity Management recognizes the line manager information for Kim and automatically assigns the business role “Marketing Manager”.

4. Day of position change
   Provisioning of role and authorization information to relevant target systems

   - User updated “Employee” “Line Manager”
   - User created “Marketing Controller”
   - User updated “Marketing Controller”
   - User updated Access to SAP ESS
   - Access to SAP MSS
   - Access to SAP CRM

HR operations

SAP ERP

SAP HCM

SAP SuccessFactors

SAP Identity Management

SAP ERP

SAP HCM

SAP CRM

SAP Portal
HR business processes as a basis: Termination

After eight years, Kim leaves the company. The day after her official assignment with the company ends, she is no longer able to access any corporate systems.

1. HR ensures that all data relevant for the employment contract termination is available, such as last day of work.

2. Event-based extraction of personnel data

3. SAP Identity Management recognizes the last day information for Kim; it automatically takes away all access rights and disables her accounts.

4. Day after termination of employment

- SAP ERP HCM: User disabled
- SAP ERP: User disabled
- SAP CRM: User disabled
- SAP Portal: User disabled
Solution in detail

Compliant identity management
Why do we need compliance within identity management?

Consistent view on current and historic **access rights**, approvals, and **policy violations**

Central management of heterogeneous environments

Integration based on standards

Compliant identity management across SAP and **heterogeneous** landscapes in one **integrated** solution

**SAP Identity Management**

**SAP Access Control**

Compliance checks

Business risk controls and mitigation
See how it works: Workflow process view

1. Request role assignment
2. Manager approval
3. Forward request for risk analysis
4. Risk analysis
5. Risk mitigation
6. Risk status
7. Provisioning to target systems
8. Notification to user and manager

SAP applications
- SAP SCM
- SAP ERP HCM
- SAP ERP
- SAP SuccessFactors
- Java
- SAP HCP
- Portal
- Active Directory
- Legacy
- E-mail
- Web app
- OS
- Database

Non-SAP applications
- …
Combining compliance with business-driven identity management

**Requirement:**
Provide automated, position-based role management while ensuring compliance

**Solution:**
- Simplify and automate role assignment
- Reduce risk through compliance checks and remediation
- Automate manual processes through integration with SAP Business Suite

1. New Hire
   - SAP ERP HCM

2. Calculate entitlements based on position
   - SAP ERP HCM

3. Compliance check
   - Remediation

4. Approve assignments
   - Yes
   - No
   - Non-SAP
   - SAP Portal
   - SAP ERP
   - SAP ERP HCM

5. Landscape
   - Line Manager

© 2019 SAP SE or an SAP affiliate company. All rights reserved. I PUBLIC
Solution in detail

Reporting
All reporting options at a glance

Basic reporting
Focus: Static, printable reports
Report creation on database level

Extended reporting with SAP Business Warehouse (SAP BW)*
Focus: Dynamic reports, offering more, highly detailed, and customizable reporting options
Data is extracted from SAP Identity Management on a regular basis (as per defined job)
Predefined report templates available, custom reports can be freely defined
Filtering, sorting, export to MS Excel, CSV, PDF, send via email, etc.

Reporting with SAP Lumira**
Focus: Customer-specific reports/analyses for identity management
Rich graphical capabilities for visualizing and utilizing reported data
Low integration and maintenance efforts
Easy extension

* SAP BW is not part of the SAP Identity Mgmt. license
** SAP Lumira, one desktop edition license is included
Option 1: Basic reporting

Application/privilege-centric
Determination of system access

User-centric
Determination of user privileges

Entry data
Current data, historical data, time stamps, modified by, audit flags

Approval data
Who approved what when?

Who had which privilege when?
Segregation of duties, Attestation

Task audit log
Determination of tasks run on user / by user

General logs
Off-the-shelf reporting tools can be used
Option 2: Extended reporting with SAP Business Warehouse

SAP BW report templates
Persons, privileges, roles and their assignments over time and for specific dates
Content-based and time-based reporting

Advanced filtering and sorting options

Access control
Roles for reporting user
(administrator, manager, owner)

Basic audit data
Who changed what

Flexibility
BEX reports
Option 3: Reporting with SAP Lumira

Customer-specific reposts/analyses for identity management

Rich graphical capabilities for visualizing and utilizing reported data

Low integration and maintenance efforts

Easy extension
Solution in detail

Password management
Password management

**Requirement:**
Reduce help desk calls related to password reset inquiries
Enable password provisioning across heterogeneous landscapes

**Solution:**
Centralize and automate password management

- Reset password
- Recover lost password
- Set new password

User

Helpdesk

SAP Identity Management

Landscape

SAP ERP

HCM

SAP ERP

Portal

Non-SAP
Solution in detail

Connectivity
Connectivity for SAP and non-SAP systems

**Databases**
- SAP HANA Database
- Microsoft SQL Server
- Microsoft Access
- Oracle database
- IBM UDB (DB2)
- MySQL
- Sybase

**Directory servers**
- Microsoft Active Directory
- IBM Tivoli Directory
- Novell eDirectory
- Oracle Directory (fka. SunOne)
- Oracle Internet Directory
- Microsoft Active Directory
- Application Mode (ADAM)
- Siemens DirX
- OpenLDAP
- eB2Boom View500 Directory Server
- CA eTrust Directory
- SAP IDM Virtual Directory Server
- Any LDAP v3 compliant directory server

**On-premise/cloud applications**
- SAP Business Suite
- SuccessFactors
- SAP Access Control (GRC)
- Lotus Domino/Notes (C API)
- Lotus Domino/Notes (Java API) for IDM8.0
- Microsoft Exchange
- RSA ClearTrust

**Technical**
- SPML
- LDAP
- ODBC/JDBC/OLE-DB
- RFC
- LDIF files
- XML files
- CSV files

...more available and possible ...
Extended connectivity capabilities
Connector to SuccessFactors Employee Central

Business process integration with SuccessFactors
- Identity propagation if initiated from SAP SuccessFactors
- Identity propagation is initiated from SAP Identity Management

Identity propagation initiated by SAP Identity Management
(role and authorization information)

Identity propagation initiated by SAP SuccessFactors
(new hire, position change, re-hire, termination)

Event-based extraction of personnel data

HR Operations

Personnel action in HR
New hire, termination, change of position etc.

Based on organizational data in HR automatic role assignment possible

Manager approves the assignment

Line Manager

At relevant date
Provisioning of role and authorization information to relevant target systems

SAP ERP
HCM

SAP SuccessFactors

SAP Identity Management

SAP ERP
HCM

SAP CRM

SAP Portal

© 2019 SAP SE or an SAP affiliate company. All rights reserved. I PUBLIC
Integration with services for SAP Cloud Platform

Existing customers of SAP Identity Management can extend their identity lifecycle management to cover cloud-based scenarios using identity provisioning and identity authentication services.

- **For on-premise landscapes**, SAP Identity Management remains the recommended solution, as it covers the on-premise expectations with respect to customization and performance.

- **For cloud systems**, the SAP Cloud Platform Identity Provisioning service is recommended. Its deployment model and simplicity better match the characteristics of cloud-based business applications. While SAP Identity Management includes a smaller set of connectors for cloud applications, the identity provisioning service is the basis for broad cloud integration allowing customers to efficiently onboard new applications.

- **In hybrid cloud and on-premise scenarios**, SAP recommends integrating SAP Identity Management with identity provisioning. Only this approach gives customers access and the maximum benefits of both worlds.
Identity and Access Management as a Service from SAP

Solution overview

**SAP Cloud Platform Identity Provisioning**
- Automatically sets up user accounts and authorizations
- Optimized for SAP cloud applications
- Re-using existing on-premise and cloud user stores
- Jointly working with the SAP Identity Management product

**SAP Cloud Platform Identity Authentication**
- Simple and secure access to web based applications
- Enterprise features like password policies and multi-factor and risk-based authentication
- On-premise user store integration
- Easy consumer and partner on-boarding via self-services

**SAP Cloud Platform Identity Access Governance**
- Access analysis
- Role design
- Access request
- Access certification
- Privilege access management

© 2019 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC
Identity and Access Governance in a hybrid landscape

SAP® Cloud Platform

SAP Cloud Identity Access Governance
- Access Analysis
- Role Design
- Access Request

SAP Cloud Platform Identity Provisioning
- Users/Groups
- Roles
- Connectors

Provisioning

End User

Workflow Self-Service

SAP Access Control
- Access Analysis
- Role Design
- Access Request

SAP Identity Management
- Users/Groups
- Roles
- Connectors

Bridge

SAP® C/4HANA
- SAP Fieldglass
- SAP Concur
- SAP SuccessFactors
- Google Cloud
- SAP Ariba
- SAP Analytics Cloud
- Microsoft Azure

CLOUD

ON-PREMISE

SAP® S/4HANA Cloud

SAP® Cloud Platform

ON-PREMISE

SAP NetWeaver

SAP Business Suite

3rd Party

...
Identity and Access Governance
Strategy and vision – evolution to the cloud

**Available**
- Focus on on-premise business applications
- IAG solution also running on-premise
- Strong IAG services and workflows
- Some limited capabilities to integrate cloud-based applications

**Available, enhancements in development**
- Supporting on-premise and cloud-based business applications
- On-premise IAG products as leading solution
- IAG cloud services used as extension to integrate cloud-based applications into the on-premise products for IAG
- Some selected new functionality available as part of the IAG cloud services

**Future plans**
- Supporting on-premise and cloud-based business applications
- IAG cloud services are the leading solution
- IAG business-process- and end-user-related capabilities available and driven by the IAG cloud services
- On-premise IAG products act as an extension to integrate on-premise applications
Out-of-the-box and third-party connectors

SAP continuously evaluates the need for additional connectors and enhances its connector portfolio in response to customer requirements.

If you are looking for a connector to an application that is not available out-of-the-box, please contact SAP consulting or one of the SAP implementation partner companies. They will be able to advise on the current planning for your specific application, or custom-create this connector for you.

SAP provides a Connector Development Toolkit (CDK) for partners and customers to develop their own connectors.

For more information about connectivity, including third-party connectors, please refer to the SAP Identity Management Connector Overview on SAP.COM.
Extended connectivity capabilities
Connector development kit 2.0

Develop connectors for non-supported target systems
Reuse Eclipse environment and standard procedures during development process
Produce traditional connector structured as a package
Solution in detail

Architecture
SAP Identity Management architecture
Eclipse based development environment

Development authorization concept
– UME based user access
– Fine grained access controls
– Multi-user environment

Harmonization of development
– JavaScript language support
– Revision-control
– Development lifecycle
– Graphical workflow design
– Configuration package concept

Web user interface administration
– Web-based management interface
– Improved usability
– Standardization
Identity virtualization
Virtual Directory Server

**Virtual Directory Server (VDS) provides**
Single consistent view and entry point for multiple distributed identity data sources
Identity information as a service for applications through standard protocols (LDAP, SPML)
Abstraction layer for underlying data stores

**Consumer only sees one standard interface**
Transform incoming LDAP requests, and connect directly to the existing data repositories while data stays within original data source and performs efficient caching

**Properties**
Real-time access to data
No need to consolidate data sources
No extra data store with quick LDAP deployment and easier, cheaper maintenance
Attribute manipulation
Name space modifications
Complex operations on-the-fly
Summary and Additional Information
Summary

SAP Identity Management is part of a comprehensive SAP security suite and covers the entire identity lifecycle and automation capabilities based on business processes.

A strong integration with SAP Access Control creates a holistic identity and access governance solution.

Extensive connectivity with SAP and non-SAP applications extends identity management to all areas of the enterprise.
Find more information
Online on SAP.COM

Visit the SAP.COM community pages for comprehensive information on SAP Identity Management, such as:

- Discussion forum, product information, documentation, training and support information, articles, blogs, WIKI, FAQs, newsletters and downloads.

### Key links for more information

**For customers and partners**

#### Key links

- SAP Cloud Trust Center: [https://www.sap.com/about/trust-center.html](https://www.sap.com/about/trust-center.html)
- SAP Innovation Discovery: [https://go.support.sap.com/innovationdiscovery](https://go.support.sap.com/innovationdiscovery)
- SAP Security Community: [https://www.sap.com/community/topics/security.html](https://www.sap.com/community/topics/security.html)
- SAP IDM Community: [https://www.sap.com/community/topics/identity-management.html](https://www.sap.com/community/topics/identity-management.html)

#### Product info on SAP.COM


#### Where to go to provide product feedback and ideas

- SAP Idea Place: [https://ideas.sap.com](https://ideas.sap.com)
- SAP User Groups: [http://www.sapusergroups.com](http://www.sapusergroups.com)
Thank you