

Identity Governance & Administration für SAP Landschaften

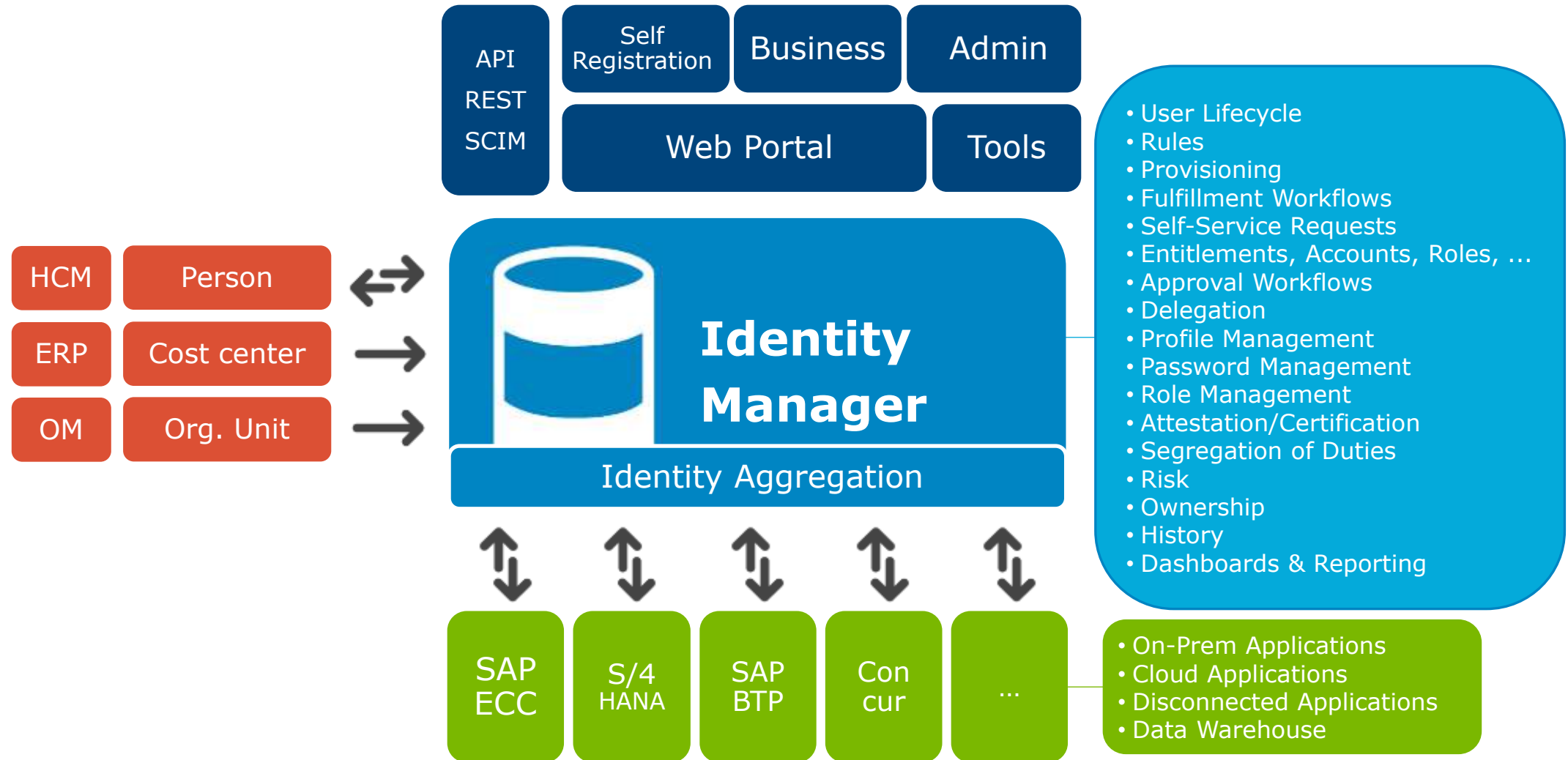
Dr. Stephan Hausmann

Halle 9-145

Agenda

- Überblick - One Identity Manager
- SAP Systeme (HR/OnPrem/Cloud)
- GRC - Governance, Risk & Compliance
- Kommentare zu Migrationen von existierenden Implementierungen

Überblick Identity Manager





SAP Systeme

SAP HCM

Display Organizational Assignment

Person: Dipl.Kfm. Ulrike Zaucker

Enterprise structure: CoCode 1000, Pers.area 1300, Cost Ctr 2100

Personnel structure: EE group 1, EE subgroup DT

Organizational plan: Position 50000083, Job key 50011879

Administrators: Group 1300, PersAdmin 00011879, PAdrAdmin 00011879

Org. Unit: 50000563, Accts Pay - D

Navigation: Organizations

- IDES AG
 - IDES Argentinien
 - IDES Australia
 - IDES Austria
 - IDES Brasilien
 - IDES Canada
 - IDES China Company
 - IDES CO
 - IDES France
 - IDES Germany
 - Corporate services (D)
 - Accounts Payable (D)

Accounts Payable (D) details:

- Department: Accounts Payable (D)
- Parent department: Finance and Administration - (D)
- Location: [Redacted]
- Manager: Zaucker, Dipl.Kfm. Ulrike (UZAUCKER)
- Role approver: [Redacted]
- Role approver (IT): [Redacted]
- Block inheritance: -

Primary assigned identities (10):

- Awad, Jasmin (JAWAD)
- Elsner, Hannelore (HELSNER)
- Gutjahr, Hanno (HGUTJAHR)
- Harmer, Andreas (AHERMES)
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Communication data overlay:

- First name: Ulrike
- Last name: Zaucker
- Middle name: [Redacted]
- Form of address: Ms
- Title: Dipl.Kfm.
- Surname prefix: [Redacted]
- Preferred name: [Redacted]
- Job description: [Redacted]
- Initials: [Redacted]
- Name at birth: [Redacted]
- Language: German [de]
- Language for value formatting: [Redacted]
- Sub-organization: [Redacted]
- Certification status: Certified
- Employee type: Employee

Kommunikationsdaten

SAP SuccessFactors HR

BestRun Org Chart

Search for actions or people

Chart Position Org Chart Company Structure Overview Directory Resources

Search for people

Mohan Kumar
4/10/22

Michael Pittman
4/3/22

Brian Kenny
Chief Information Officer (C...)
1/2

Christine Dolan
Chief Human Resources Officer
5/23 - 7 Matrix

James Patrick
VP Shared Services
5/5

Nicole Anderson
Executive Assistant

Michael Pittman
Global Operations (50007725)

Cleveland (1710-2013)

8:34 AM

Identity
Kumar, Mohan (890223) (890223)

Form of address

Full name Kumar, Mohan (890223)

Phone (1) 212 555-4222

Mobile phone

Fax

Building 1710-2001

Floor

Room A

Central user account 890223

Central SAP user account KUMARM

Default email address mohan.kumar@bestrunsap.com

Primary location Corporate - US-Philadelphia (1710-2001)

Primary department BestRun Corporation (1)

Primary cost center US10_M2 (USA Executive BoardUS10_M2)

Primary business role

Manager

VIP -

Permanently deactivated -

External -

Identity type Primary identity

One Identity Manager accountability (5)

Department manager: BestRun Corporation (1)(1)

Manager: Akane, Audrey (69121)

Manager: Amos, Eileen (890274)

Manager: Pittman, Michael (80281)

Identity
Pittman, Michael (80281) (80281)

Form of address

Full name Pittman, Michael (80281)

Phone (1) 215 555-0722

Mobile phone

Fax

Building 1710-2013

Floor

Room A

Central user account 80281

Central SAP user account PITTMANM

Default email address Michael.Pittman@bestrunsap.com

Primary location Cleveland (1710-2013)

Primary department Global Operations (50007725)

Primary cost center US10_M2 (USA Executive BoardUS10_M2)

Primary business role

Manager **Kumar, Mohan (890223) (890223)**

VIP -

Permanently deactivated -

External -

Identity type Primary identity

One Identity Manager accountability (5)

Department manager: **BestRun Corporation \Global Operations (50007725)(50007725)**

Manager: Anderson, Nicole (80202)

Manager: Dolan, Christine (80279)

Manager: Kenny, Brian (BKENNY)

Manager: Patrick, James (103073)

Kommunikationsdaten

Templates: Data Mapping (SuccessFactors HR)

The screenshot displays the One Identity Manager interface with two schema comparison panes. The left pane shows the 'Person (all)' schema from 'dbsrv.demolab.com\OneIM', and the right pane shows the 'SCIM Employees (all)' schema from 'Cross-Domain Identity Mana...'. The central area is divided into 'Object matching rules' and 'Property mapping rules'.

Object matching rules:

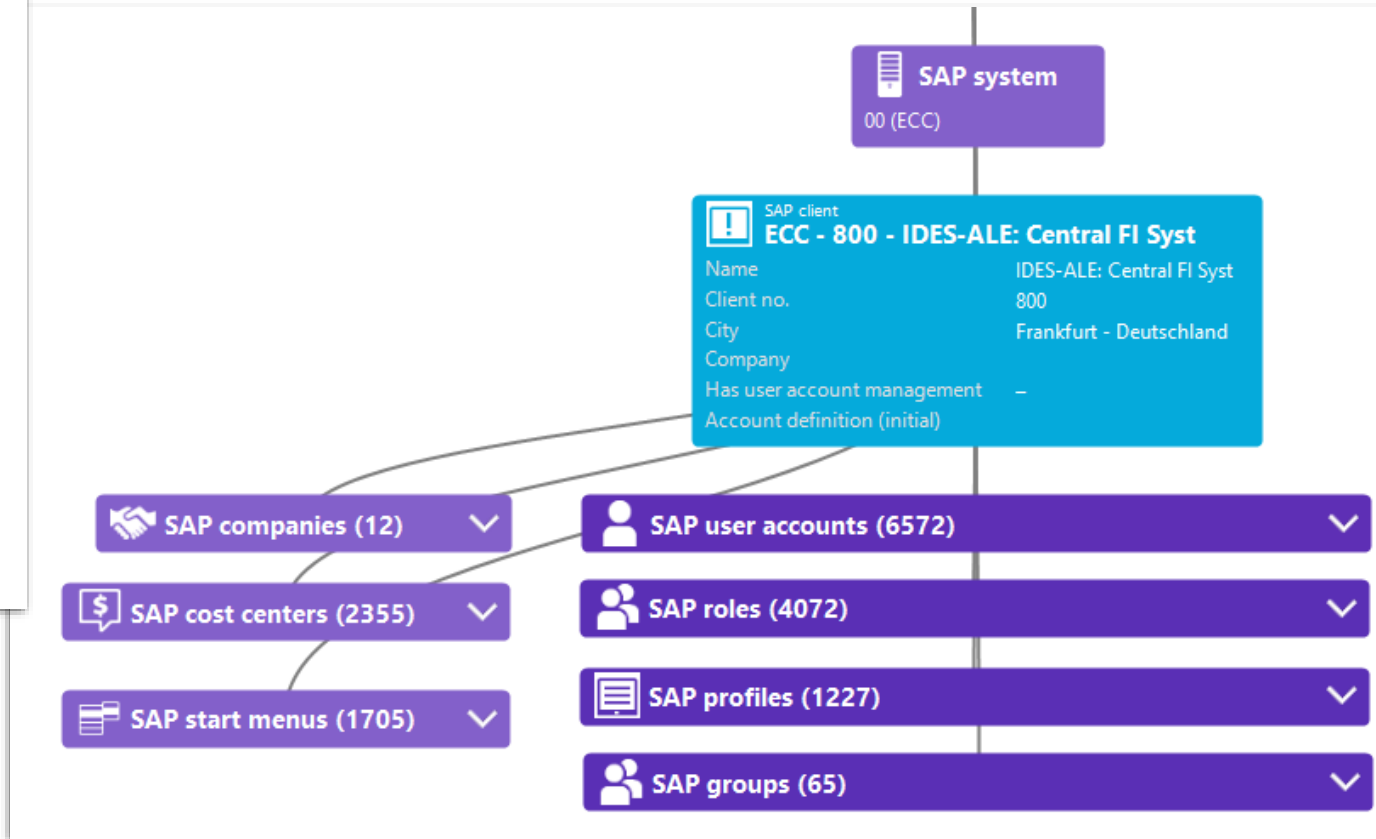
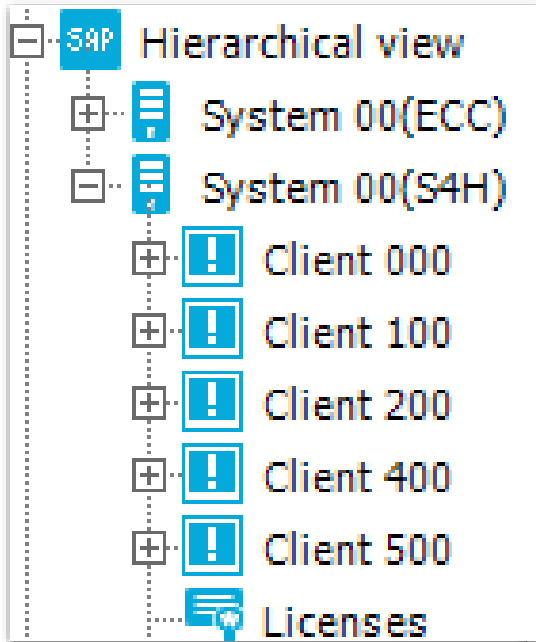
Schema property in One Identity Manager	Information	Schema property in the target system
CentralAccount	Primary rule	id
DistinguishedName	Alternate rule	vrtdistinguishedName

Property mapping rules:

Schema property in One Identity Manager	Information	Schema property in the target system
CanonicalName		vrtpcanonicalName
CentralAccount		id
DefaultEmailAddress		emails~value
DistinguishedName		vrtdistinguishedName
FirstName		name~givenName
FormerName		userName
ImportSource		sourceSystem
InternalName		userId
LastName		name~familyName
Phone		phoneNumbers~businessPhone
PhoneMobile		phoneNumbers~cellPhone
PreferredName		name~formatted
Title		title
VRT_CHSConnectorRoot		vrtparentDn
vrtpCostCentersMapping		costCenter
vrtpDepartmentsMapping		department
vrtpLocationsMapping		location
vrtpPersonHead		managerId

Red boxes highlight the 'DefaultEmailAddress' and 'LastName' rows in the Property mapping rules table, showing their mapping to 'emails~value' and 'name~familyName' respectively.

SAP ECC und S/4HANA OnPrem

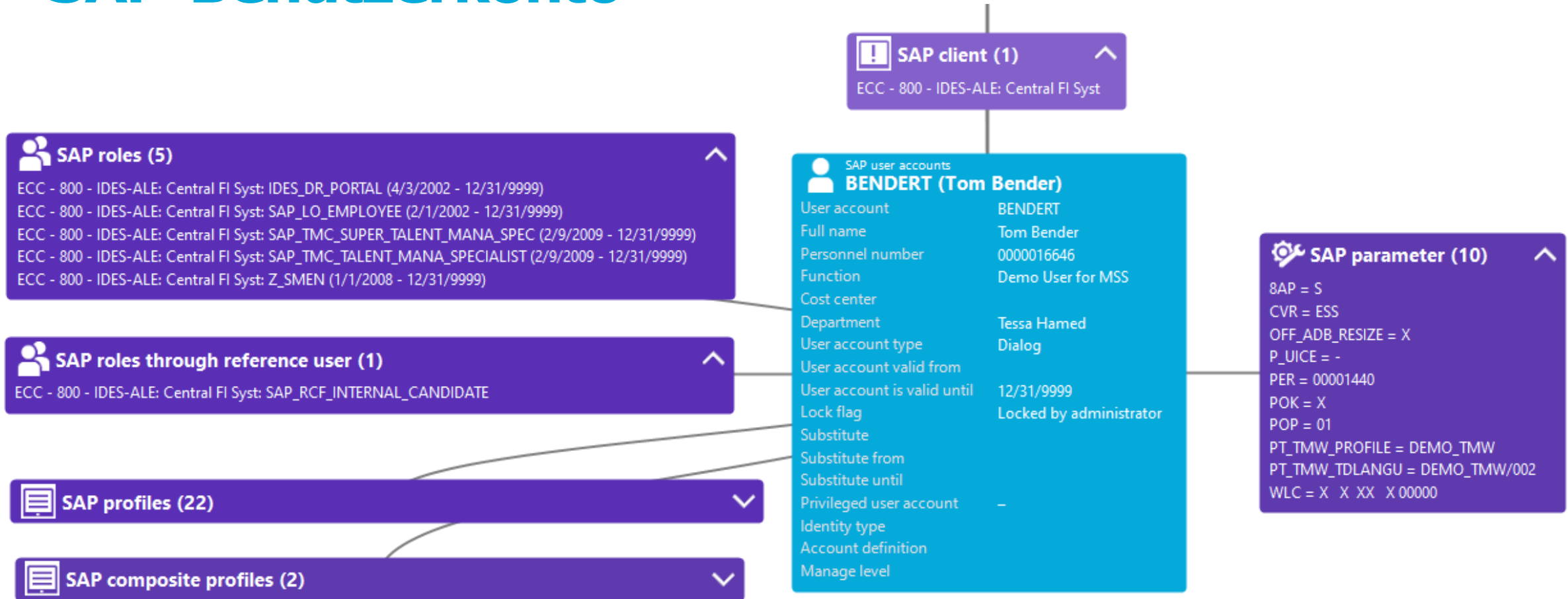


WHITE PAPERS

[How to manage SAP-User Accounts and Access Rights with Identity Manager](#)

Identity Manager helps you set up and manage SAP user accounts, groups, roles, profile assignments and transactions. Get our white paper to learn ...

SAP-Benutzerkonto



Master und abgeleitete SAP Rollen

Pflege: 0 ungepflegte Orgebenen, 0 offene Felder, Status: unverändert

X:N:MM:IM_GOODS_MOV_INFO:00000 MM-IM Bestandsführung Information

- Standard Anwendungsübergreifende Berechtigungsobjekte
- Gepflegt Basis - Administration
- Standard Finanzwesen
- Gepflegt Materialwirtschaft - Bestandsführung und Inventur
 - Gepflegt Reservierungen: Bewegungsart
 - Standard Reservierungen: Werk
 - Aktivität **Anzeigen**
 - Werk
 - Gepflegt Materialbelege: Bewegungsart
 - Gepflegt Warenbewegungen: Lagerort
 - Standard Materialbelege: Werk
 - Aktivität **Anzeigen**
 - Werk

Anzeigen von Rollen

Rolle: **X:N:MM:IM_GOODS_MOV_INFO:DE001**

Beschreibung

Beschreibung Menü Berechtigungen Benutzer MiniApps Personalisierung

Verwaltungsinformation Vererbung der Transaktionen

Benutzer	Angelegt	Geändert	Abteilen aus Rolle
IDADMIN	25.01.2024	25.01.2024	X:N:MM:IM_GOODS_MOV_INFO:00000

MM-IM Bestandsführung Information

Pflege: 0 ungepflegte Orgebenen, 0 offene Felder, Status: unverändert

X:N:MM:IM_GOODS_MOV_INFO:DE001 X:N:MM:IM_GOODS_MOV_INFO:DE001

- Standard Anwendungsübergreifende Berechtigungsobjekte
- Gepflegt Basis - Administration
- Standard Finanzwesen
- Gepflegt Materialwirtschaft - Bestandsführung und Inventur
 - Gepflegt Reservierungen: Bewegungsart
 - Standard Reservierungen: Werk
 - Aktivität **Anzeigen 0007**
 - Werk
 - Gepflegt Materialbelege: Bewegungsart
 - Gepflegt Warenbewegungen: Lagerort
 - Standard Materialbelege: Werk
 - Aktivität **Anzeigen 0007**
 - Werk

Bestellungen von Rollen mit Kontext – Werk/Land

Bestelldetails ✕

i Geben Sie für die folgenden Produkte zusätzliche Informationen an. Für alle anderen Produkte müssen Sie keine zusätzlichen Informationen angeben.
Sie können sich auch entscheiden, einzelne Produkte nicht in den Einkaufswagen zu legen. ✕

? Rolle mit Kontext Accounting, Bart (BACCOUNTING) ⤴

Context Type *
Land ✕

Kontext *
Deutschland ✕

Rolle *
MM-Goods Movement Information ✕

Nicht in Einkaufswagen legen Übernehmen



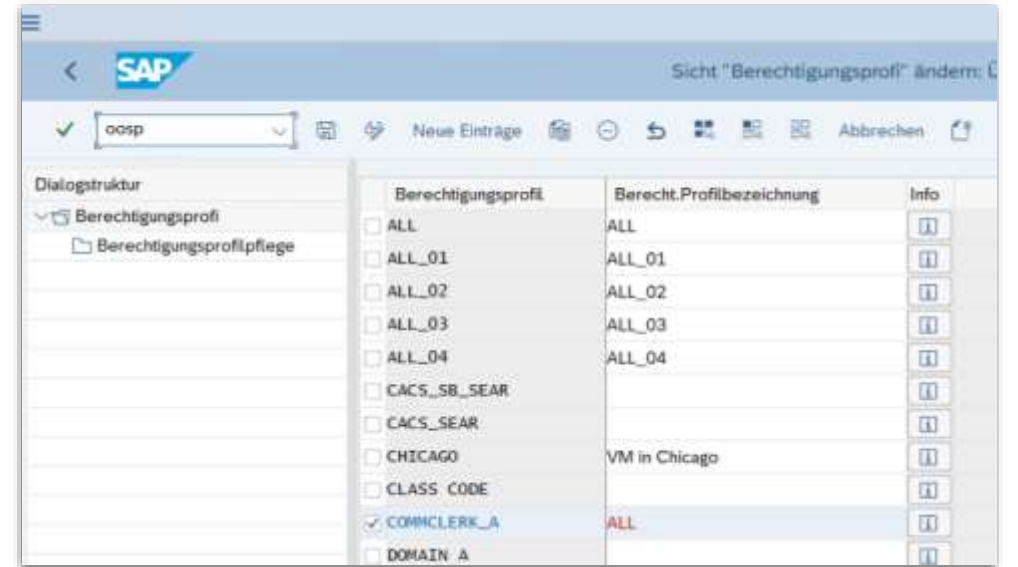
WHITE PAPERS

Context-based requests for Identity Manager

This white paper offers techniques and features of Identity Manager that simplify Context assignment within the world of SAP roles.

Weiteres

- Strukturelle Berechtigungen im HCM (OOSP)
- BI Analyseberechtigungen (RSECADMIN)
- Hana DB
 - Datenbank Konten
 - Datenbank Tabellen

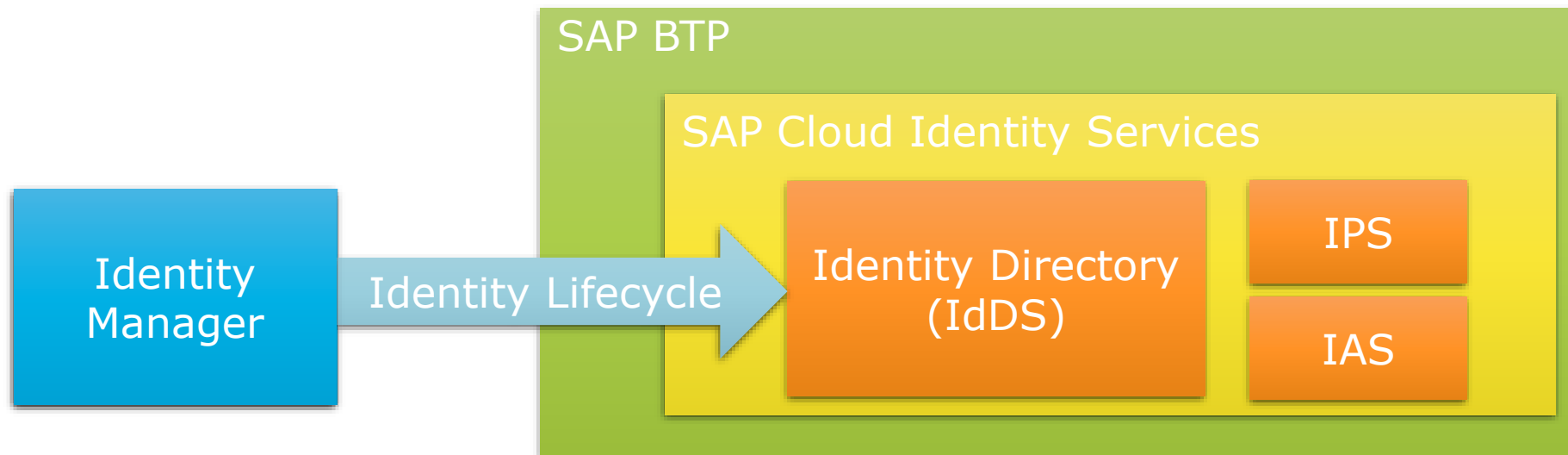


Integration mit SAP Cloud Identity Services

- **“Cloud leading Identity Lifecycle”**

“This reference architecture describes the identity lifecycle flows for SAP applications via the SAP Cloud Identity Services.”

<https://discovery-center.cloud.sap/refArchDetail/ref-arch-cloud-leading-identity-lifecycle>



SAP Cloud Identity Service

SAP Cloud Identity Services Trial-US-East

Home | Users & Authorizations | Identity Provisioning | Application

Users & Authorizations

- User Management: 2
- Groups: 1

Identity Provisioning

- Source Systems: 0
- Target Systems: 1

SAP Cloud Identity Services Trial-US-East

Home | Users & Authorizations | Identity Provisioning | Applications & Resources | Identity Providers | Monitoring & Reporting

Groups

Show Filter Bars | Import

Groups: Search by Group ID, Display Name or Name

Groups (1) | Create | Delete | Settings

Display Name	Application Name	Type
Test Group		User Group

Group ID: 33e53a2f-4da5-4e3a-8751-fcdd7ed1ab22

Test Group

Test Group

Group ID: 33e53a2f-4da5-4e3a-8751-fcdd7ed1ab22 | Display Name: Test Group | Description: First Test Group

Type: User Group | Name: Test Group

User Members

Users (1 out of 1) | Search by SCIM ID, Login Name or Email | + Add | Remove | Settings

First Name	Last Name	Email	Login Name	SCIM ID
Test	User	test.user@demolab.com	test.user	13351be3-ff36-405d-b85e-9a19149c5d58

SCIM und Template für SAP Identity Directory

Create system connection...

Target product selection
Change the connector's behavior to adjust to target product singularities (for example, HTTP request style)

Selection of a product specific serializer (creating HTTP requests)

Target Product: **SCIM Core V 2.0**

- SCIM Core V 2.0
- One Identity Starling Connect
- SCIM SAP Cloud IDS

Mapping and Synchronization of Dayforce system data to Identity Manager

One Identity Starling Connect SuccessFactors HR

Mapping and Synchronization of SuccessFactors HR system data to Identity Manager

One Identity Starling Connect Workday HR

Mapping and Synchronization of Workday HR system data to Identity Manager

SCIM Synchronization

System for Cross-Domain Identity Management synchronization

SCIM synchronization of the SAP Cloud AUM application

Synchronization of an SAP Cloud AUM application via SAP Cloud Identity Services (with default schema)

One Identity Starling Connect synchronization

System for Cross-Domain Identity Management synchronization using One Identity Starling Connect.

Create blank project

Use this option if you do not want to apply a project template. This add an empty synchronization project for the target system. Define synchronization behavior with the Synchronization Editor.

Back Next Cancel

Cloud target systems
Cloud Identity Domain SAP IdDS
Display name: Cloud Identity Domain SAP IdDS

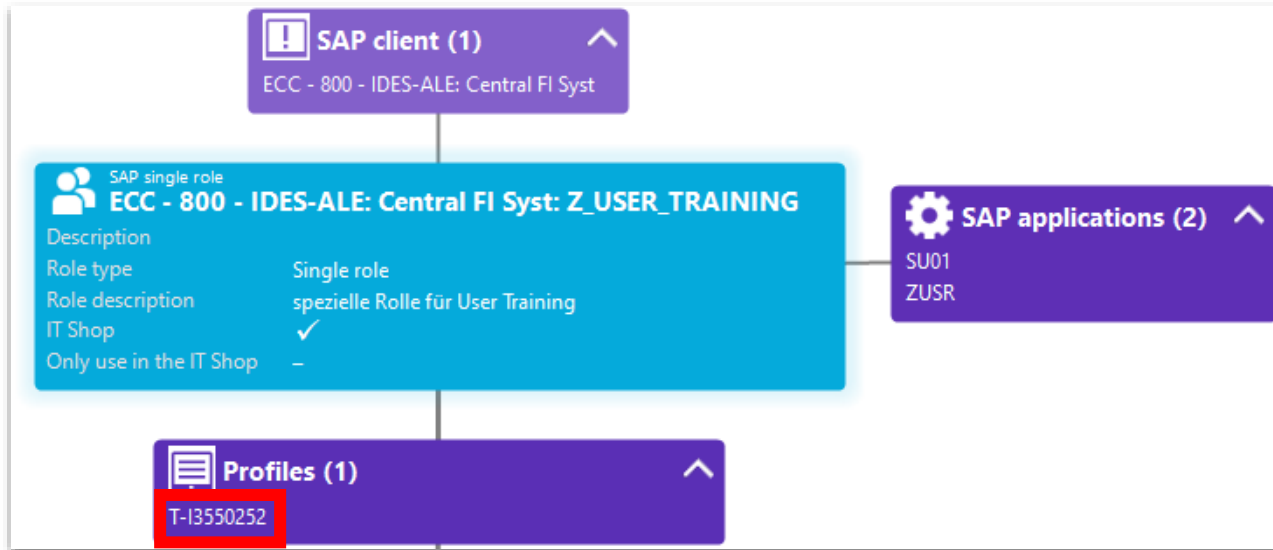
Cloud group
Test Group
Display name: Test Group
Description: First Test Group
IT Shop: -
Only use in the IT Shop: -
Container

User accounts (1)
test.user (Test User)



GRC - Governance, Risk & Compliance

Berechtigungsobjekte in SAP: Basis für SoD



Authorization	Value	Description
T-13550252		
ACT_GROUP	*	Role Name
ACTVT	03	Activity
Business Address Services: Address Type 1 (Org. Addresses)		
ACTVT	06	Activity
ACTVT	03	Activity
ACTVT	02	Activity
ACTVT	01	Activity
ADGRP	BC01	Address Group (Key) (Business Address Services)
C calls in ABAP programs		
ACTVT	16	Activity
CFUNCNAME	*	Name of a CALLable C routine
PROGRAM	*	Program Name with Search Help
HR: Transaction codes		
TCD	SU01	Transaction Code
SAPoffice: Office User Attribute		
OFFADMI	*	Text field length 15: authorization check
Transaction Code Check at Transaction Start		
TCD	SU01	Transaction Code
TCD	ZUSR	Transaction Code
User Master Maintenance: Authorization Profile		
ACTVT	08	Activity
ACTVT	03	Activity
PROFILE	*	Auth. profile in user master maintenance
User Master Maintenance: Authorizations		
ACTVT	08	Activity
ACTVT	03	Activity
AUTH	*	Authorization name in user master maintenance
OBJECT	*	Authorization Object
User Master Maintenance: System for Central User Maintenance		
ACTVT	78	Activity
SUBSYSTEM	*	Receiving system for central user administration

Einsatz von SoD Regeln

- Prüfung der importierten SAP-Rollen auf Konflikte
- Prüfung der importierten SAP-Konten auf Konflikte
- Prüfung von Fachrollen und deren Inhalten
- Prüfung beim Antrag
 - von SAP-Rollen und Fachrollen für Identitäten
 - von SAP-Rollen für Fachrollen
 - Antrag mit SAP GRC Anfrage



WHITE PAPERS

SAP GRC Framework Integration with One Identity Manager

SAP Cloud Identity Access Governance (SAP IAG) and SAP Access Control (SAP AC) are two powerful solutions from SAP to address critical governance,...

Risiko,

ONE IDENTITY One Identity Manager Web Portal

Bestellungen ▾ Attestierung ▾ Compliance ▾ Verantwortlichkeiten ▾ Datenv...

Offene Bestellungen i

Suchen

<input type="checkbox"/> Produkt	Status der Bestellung	Bestelldatum		
<input type="checkbox"/> Z_SAP_AUDITOR Empfänger: Einkauf, Dieter	Bestellt	10/9/2024	⚠ Regelverletzung	⊘ Ablehnen ✓ Genehmigen ⊗ Empfehlung



4

Kommentare zu Migrationen von existierenden Implementierungen

Kommentare zu Migrationen

- Alter Wein in neuen Schläuchen?
- Existierende Prozesse neu beleuchten?
- Gehört das alles in IGA?
- ...

Ratgeber für Identity Governance und Administrationsprojekte

<https://www.security-insider.de/ratgeber-fuer-identity-governance-und-administrationsprojekte-a-c0e993dd40307fbc21372f981807c6c4/>

Halle 9-145

