One Identity Manager 8.1.4

Administrationshandbuch für die Anbindung einer SAP R/3-Umgebung

Legende

WARNUNG: Das Symbol WARNUNG weist auf ein potenzielles Risiko von Körperverletzungen oder Sachschäden hin, für das Sicherheitsvorkehrungen nach Industriestandard empfohlen werden. Dieses Symbol ist oft verbunden mit elektrischen Gefahren bezüglich Hardware.

VORSICHT: Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.

One Identity Manager Administrationshandbuch für die Anbindung einer SAP R/3-Umgebung
Aktualisiert - 19. Oktober 2020, 08:33 Uhr
Version - 8.1.4

Inhalt

Verwalten einer SAP R/3-Umgebung

Der One Identity Manager bietet eine vereinfachte Administration der Benutzer einer SAP R/3-Umgebung. Dabei konzentriert sich der One Identity Manager auf die Einrichtung und Bearbeitung von Benutzerkonten sowie die Gruppen-, Rollen- und Profilzuweisungen. Externe Kennungen und Parameter können ebenfalls an Benutzerkonten zugewiesen werden. Zusätzlich werden die benötigten Daten zur Systemvermessung abgebildet. Im One Identity Manager werden die Daten zur Systemvermessung zur Verfügung gestellt, die eigentliche Vermessung erfolgt jedoch in der SAP R/3-Umgebung.

Im One Identity Manager werden die Personen eines Unternehmens mit den benötigten Benutzerkonten versorgt. Dabei können Sie unterschiedliche Mechanismen für die Verbindung der Personen mit ihren Benutzerkonten nutzen. Ebenso können Sie die Benutzerkonten getrennt von Personen verwalten und somit administrative Benutzerkonten einrichten.

Um den Benutzerkonten die benötigten Berechtigungen zur Verfügung zu stellen, werden im One Identity Manager Gruppen, Rollen und Profile abgebildet. Gruppen, Rollen und Profile können zu Produkten zusammengestellt und an Personen zugewiesen werden. Der One Identity Manager stellt sicher, dass für alle Benutzerkonten einer Person die entsprechenden Gruppenmitgliedschaften erzeugt werden.

Werden Benutzerkonten in der SAP R/3-Umgebung über die Zentrale Benutzerverwaltung (ZBV) administriert, kann den Benutzerkonten im One Identity Manager der Zugriff auf die Tochtersysteme gewährt und entzogen werden.

Architekturüberblick

Für die Verwaltung einer SAP R/3-Umgebung spielen im One Identity Manager folgende Server eine Rolle:

- SAP R/3-Anwendungsserver

  Anwendungsserver, gegen den die Synchronisation läuft. Der Synchronisationsserver verbindet sich gegen diesen Server, um auf die Objekte der SAP R/3-Umgebung zuzugreifen.

- SAP R/3-Datenbankserver

  Server, auf dem die Datenbank der SAP R/3-Anwendung installiert ist.
- Synchronisationsserver

  Synchronisationsserver für den Abgleich zwischen der One Identity Manager-Datenbank und der SAP R/3-Umgebung. Auf diesem Server ist der One Identity Manager Service mit dem SAP R/3 Konnektor installiert. Der Synchronisationsserver verbindet sich gegen den SAP R/3-Anwendungsserver.
- SAP R/3-Router

  Router, der dem SAP Konnektor einen Netzwerkport zur Kommunikation mit dem SAP R/3-Anwendungsserver bereitstellt.
- SAP R/3-Message-Server

  Server, mit dem der SAP R/3 Konnektor beim Login kommuniziert, wenn keine direkte Kommunikation mit den Anwendungsservern erlaubt ist.

Der SAP R/3 Konnektor des One Identity Manager führt die Synchronisation und Provisionierung der Daten zwischen der SAP R/3-Umgebung und der One Identity Manager-Datenbank aus. Der SAP R/3 Konnektor nutzt den SAP Connector for Microsoft .NET (NCo 3.0) für 64-Bit-Umgebungen für die Kommunikation mit dem Zielsystem.

Für den Abgleich der Informationen zwischen der One Identity Manager-Datenbank und der SAP R/3-Umgebung sorgt der One Identity Manager Service. Zwingende Voraussetzung für die Synchronisation ist die Installation des Application Server ABAP. Eine SAP R/3-Umgebung, die ausschließlich auf Application Server Java basiert, kann mit dem SAP Konnektor nicht angesprochen werden.

Abbildung 1: Architektur für die Synchronisation - direkte Kommunikation

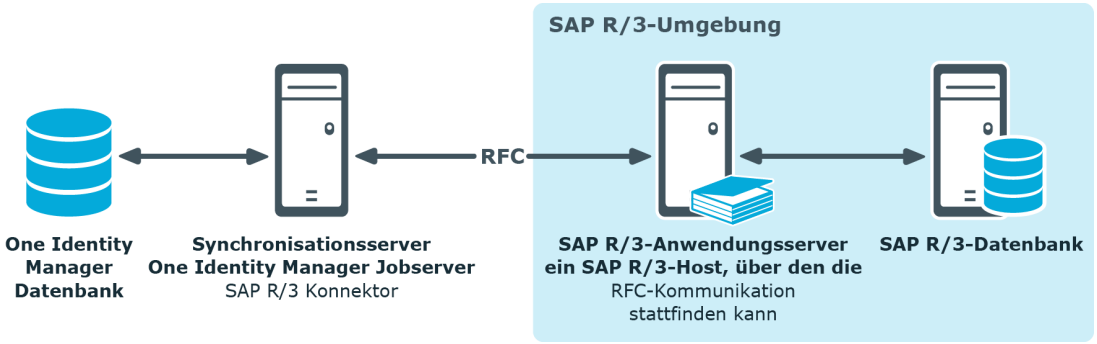


Abbildung 2: Architektur für die Synchronisation - Kommunikation über Message-Server

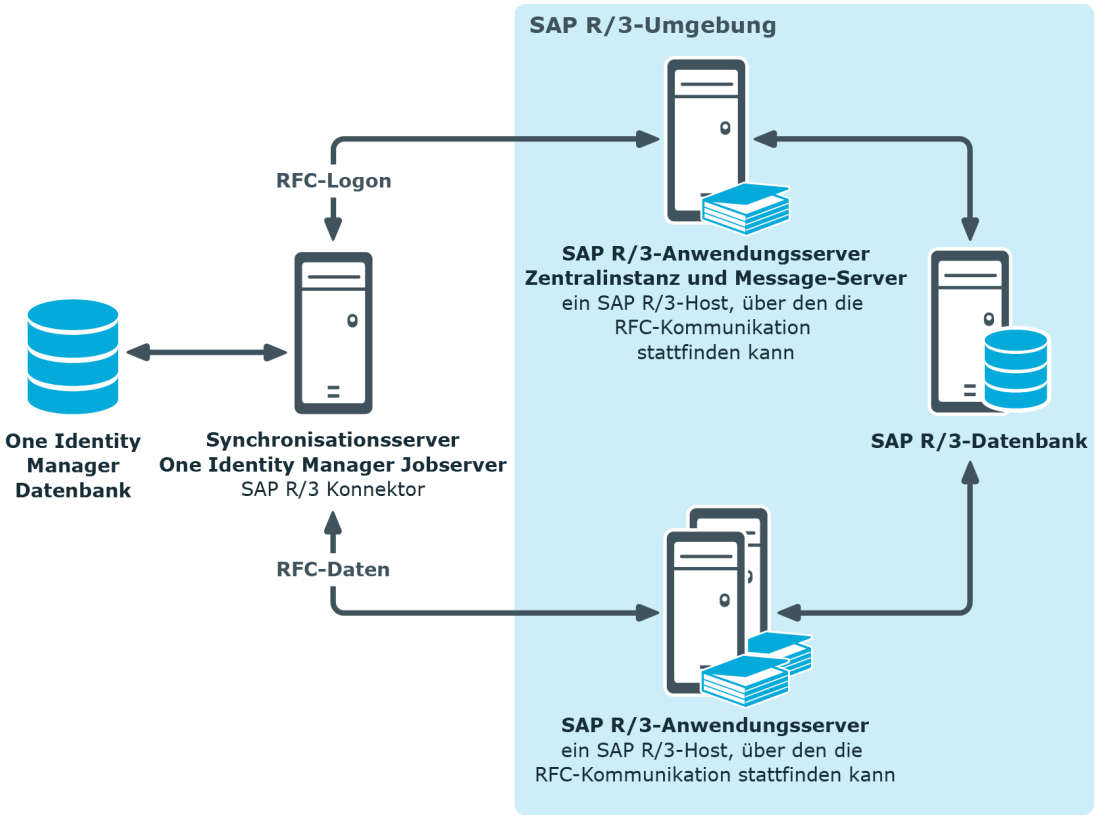
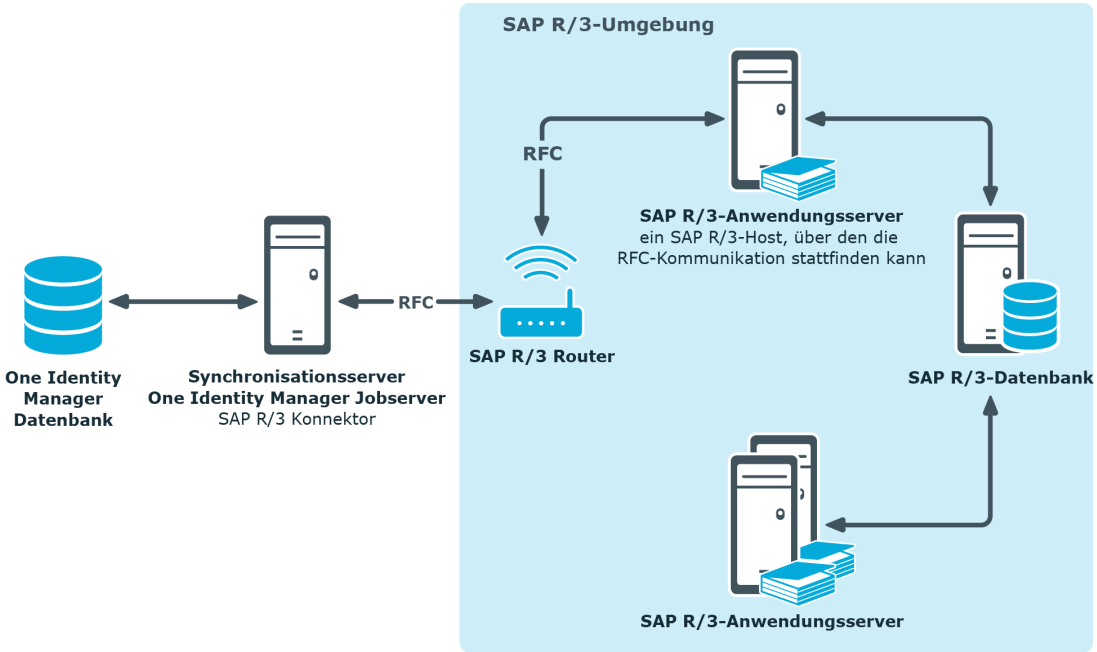


Abbildung 3: Architektur für die Synchronisation - Kommunikation über Router



One Identity Manager Benutzer für die Verwaltung einer SAP R/3-Umgebung

In die Einrichtung und Verwaltung einer SAP R/3-Umgebung sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Zielsystemadministratoren	Die Zielsystemadministratoren müssen der Anwendungsrolle **Zielsysteme | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen. • Legen die Zielsystemverantwortlichen fest. • Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein. • Legen fest, welche Anwendungsrollen für Zielsystemverantwortliche sich ausschließen. • Berechtigen weitere Personen als Zielsystemadministratoren. • Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | SAP R/3** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Systemberechtigungen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den

Benutzer	Aufgaben
	Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.
One Identity Manager Administratoren	• Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.
Administratoren für den IT Shop	Die Administratoren müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Systemberechtigungen an IT Shop-Strukturen zu.
Administratoren für Organisationen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Organisationen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zu.
Administratoren für Geschäftsrollen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Geschäftsrollen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Systemberechtigungen an Geschäftsrollen zu.

Einrichten der Synchronisation mit einer SAP R/3-Umgebung

Der One Identity Manager unterstützt die Synchronisation mit SAP Systemen in den folgenden Versionen:

- SAP Web Application Server 6.40
- SAP NetWeaver Application Server 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40, 7.40 SR 2, 7.41, 7.50, 7.51, 7.52 und 7.69
- SAP ECC 5.0 und 6.0
- SAP S/4HANA On-Premise-Edition

Für alle genannten Versionen wird die Zentrale Benutzerverwaltung unterstützt.

HINWEIS: Zwingende Voraussetzung für die Synchronisation ist die Installation des Application Server ABAP. Eine SAP R/3-Umgebung, die ausschließlich auf Application Server Java basiert, kann mit dem SAP Konnektor nicht angesprochen werden.

Um die Objekte einer SAP R/3-Umgebung initial in die One Identity Manager-Datenbank einzulesen

1. Stellen Sie in der SAP R/3-Umgebung ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Spielen Sie das One Identity Manager Business Application Programming Interface in das SAP R/3-System ein.
3. Die One Identity Manager Bestandteile für die Verwaltung von SAP R/3-Umgebungen sind verfügbar, wenn der Konfigurationsparameter "TargetSystem\SAPR3" aktiviert ist.
    - Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.
    - Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.
4. Laden Sie die Installationsquellen für den SAP .Net Connector for .NET 4.0 on x64, mindestens Version 3.0.15.0 herunter.

5. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
6. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Detaillierte Informationen zum Thema

- Benutzer und Berechtigungen für die Synchronisation mit einer SAP R/3-Umgebung auf Seite 15
- Einspielen des One Identity Manager Business Application Programing Interface auf Seite 18
- Einrichten des Synchronisationsservers auf Seite 19
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines SAP Mandanten auf Seite 23

Benutzer und Berechtigungen für die Synchronisation mit einer SAP R/3-Umgebung

Bei der Synchronisation des One Identity Manager mit einer SAP R/3-Umgebung spielen folgende Benutzer eine Rolle.

Tabelle 2: Benutzer für die Synchronisation

Benutzer	Berechtigungen
Benutzerkonto des One Identity Manager Service	Das Benutzerkonto für den One Identity Manager Service benötigt die Rechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Rechte vergeben, Verzeichnisse und Dateien anlegen und bearbeiten. Das Benutzerkonto muss der Gruppe **Domänen-Benutzer** angehören. Das Benutzerkonto benötigt das erweiterte Benutzerrecht **Anmelden als Dienst**. Das Benutzerkonto benötigt Rechte für den internen Webservice. HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so können Sie die Rechte für den internen Webservice über folgenden Kommandozeilenaufruf vergeben: `netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"`

Benutzer	Berechtigungen
	Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis. In der Standardinstallation wird der One Identity Manager installiert unter: • `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen) • `%ProgramFiles%\One Identity` (auf 64-Bit Betriebssystemen)
Benutzer für den Zugriff auf das Zielsystem	Für eine vollständige Synchronisation von Objekten einer SAP R/3-Umgebung mit der ausgelieferten One Identity Manager Standardkonfiguration stellen Sie ein Benutzerkonto bereit, das die folgenden Berechtigungen besitzt. Benötigte Berechtigungsobjekte und ihre Ausprägungen: • S_TCODE mit mindestens den Transaktionscodes SU01, SU53, PFCG • S_ADDRESS1 (Address Services) mit den Aktivitäten 01, 02, 03, 06 und den zulässigen Adressgruppen (mindestens "BC01") • S_USER_AGR (Rollenpflege) mit den Aktivitäten 02, 03, 22, 78 eventuell mit Einschränkung des Namensbereiches (z. B. "Z*") • S_USER_GRP (Gruppenpflege) mit den Aktivitäten 01, 02, 03, 22 • S_USER_AUT (Berechtigungen) mit den Aktivitäten 03, 08 • S_USER_PRO (Profile) mit den Aktivitäten 01, 02, 03, 22 • S_USER_SAS (Systemspezifische Zuordnungen) mit den Aktivitäten 01, 06, 22 • S_RFC (Berechtigungsprüfung bei RFC-Zugriff) mit der Aktivität 16 mindestens für die Funktionsgruppen ZVI, /VIAENET/ZVI0, /VIAENET/ZVI_L, /VIAENET/Z_HR, SU_USER, SYST, SDTX, RFC1, RFC_METADATA, SDIFRUNTIME, SYSU, SUSO • S_TABU_DIS (Tabellenpflege über Standardtools wie SM30) mit der Aktivität 03 Neben den aufgeführten Berechtigungen muss das Benutzerkonto alle durch den mitgelieferten Transport eingespielten Berechtigungsobjekte der Berechtigungsklassen "ZVIH_AUT", "ZVIA_AUT" und "ZVIL_AUT" erhalten. Für die Synchronisation einer Zentralen Benutzerverwaltung werden für den Zugriff auf die Tochtersysteme zusätzlich folgende Berechtigungsobjekte benötigt:

Benutzer	Berechtigungen
	• S_RFC mit der Funktionsgruppe SUU6 • S_TCODE mit dem Transaktionscode SU56
Benutzer für den Zugriff auf die One Identity Manager-Datenbank	Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer **Synchronization** bereitgestellt.

TIPP: Die standardmäßig ausgelieferte Transportdatei "SAPROLE.zip" enthält einen Transport mit einer Rolle, die das Berechtigungsobjekt des Bausteins bereits besitzt. Diese Rolle kann dem Benutzerkonto zugewiesen werden. Die Transportdatei befindet sich auf dem One Identity Manager-Installationsmedium im Verzeichnis `Modules\SAP\dvd\AddOn\Bapi`.

Die genannten Berechtigungen werden benötigt, damit der SAP R/3 Konnektor sowohl lesend als auch schreibend auf das SAP R/3-System zugreifen kann. Soll nur ein lesender Zugriff erlaubt werden, so empfehlen wir die Einrichtung eines Profils, welches zwar die Ausführungsberechtigungen auf die Transaktionen SU01 und PFCG zur Verfügung stellt, allerdings auf Aktivitäts- oder Feldebene das Schreiben verhindert.

Um weitere Informationen auszulesen, benötigt das Benutzerkonto den Benutzertyp "Dialog", "Kommunikation" oder "System".

HINWEIS: Die SAP R/3-Versionen bis einschließlich SAP Web Application Server 6.40 unterscheiden bei der Angabe von Benutzer und Kennwort nicht zwischen Groß- und Kleinschreibung. Ab SAP NetWeaver Application Server 7.0 gilt dies für Kennworte nicht mehr. Kennworte sind "case sensitiv".

Alle SAP-eigenen Werkzeuge, die bis SAP Web Application Server 6.40 ausgeliefert wurden, außer der SAP GUI (RFC-SDK, SAP .Net Connector), wandeln deshalb das Kennwort vor der Übertragung zum SAP R/3-System in Großbuchstaben um. Für das Benutzerkonto, mit welchem sich der SAP .Net Connector am SAP R/3-System authentifizieren soll, muss ein Kennwort in Großbuchstaben gesetzt werden. Danach kann mit allen gewohnten Werkzeugen per RFC auf SAP NetWeaver Application Server 7.0 zugegriffen werden.

Verwandte Themen

- Referenzierte SAP R/3-Tabellen und BAPI-Aufrufe auf Seite 231

Einspielen des One Identity Manager Business Application Programing Interface

HINWEIS: Das Business Application Programming Interface des One Identity Manager ist zertifiziert.

Zertifikate:

- Integration with SAP S/4HANA
- Powered by SAP NetWeaver

Ausführliche Informationen finden Sie unter https://www.sapappcenter.com/apps/5513#!overview.

Um mit dem One Identity Manager auf die Daten und Geschäftsprozesse der SAP R/3-Umgebung zuzugreifen, muss das mitgelieferte Business Application Programming Interface (BAPI) in das SAP R/3-System eingespielt werden. Die erforderlichen Transportdateien finden Sie auf dem One Identity Manager-Installationsmedium im Verzeichnis `Modules\SAP\dvd\AddOn\Bapi`.

TIPP: Anstelle der Transportdatei `SAPTRANSPORT_70.ZIP` können Sie auch das Assembly Kit-Paket `T070020759523_0000006.PAT` installieren. Weitere Informationen finden Sie unter Deinstallieren von BAPI-Transporten auf Seite 19.

Installieren Sie die Transporte des BAPI in folgender Reihenfolge:

Tabelle 3: BAPI-Transporte

	Transport	Erläuterung
1	SAPRepository.zip	Erstellt die /VIAENET/-Umgebung im Repository des SAP Systems.
2	SAPTable.zip	Definiert die Tabellenstruktur für /VIAENET/USERS im Dictionary des SAP Systems.
3	SAPTRANSPORT_70.ZIP	Enthält die Funktionen, die in der /VIAENET/-Umgebung definiert sind. Wählen Sie das für Ihr SAP System passende Transportpaket aus. Archivverzeichnis UNICODE: Transporte für Systeme, die Unicode unterstützen; Transport von Kopien Archivverzeichnis NON_UNICODE: Transporte für Systeme, die kein Unicode unterstützen Archivverzeichnis UNICODE_WORKBENCH: Transporte für Systeme, die Unicode unterstützen; Workbench-Transport

Aktivieren Sie für den Transport die folgenden Importoptionen:

- Originale überschreiben
- Objekte in unbestätigten Reparaturen überschreiben
- Nicht passende Komponentenversion ignorieren

Daneben nutzt der SAP R/3 Konnektor weitere BAPIs des SAP R/3-Systems. Weitere Informationen finden Sie unter Referenzierte SAP R/3-Tabellen und BAPI-Aufrufe auf Seite 231.

Deinstallieren von BAPI-Transporten

Mit dem SAP Add-On Assembly Kit unterstützt SAP die Deinstallation eines BAPI. Dafür wird ein deinstallierbares Assembly Kit-Paket bereitgestellt.

Voraussetzungen

- SAP NetWeaver Application Server 7.00 oder höher
- SAP ECC 6.0
- SAP Add-On Assembly Kit 5.0 oder höher
- Unicode wird unterstützt.

Um einen BAPI-Transport später deinstallieren zu können

- Installieren Sie das Assembly Kit-Paket `T070020759523_0000006.PAT` anstelle der Transportdatei `SAPTRANSPORT_70.ZIP`.

  Das Paket finden Sie auf dem One Identity Manager-Installationsmedium im Verzeichnis `Modules\SAP\dvd\AddOn\Bapi`.

Das Paket enthält die Funktionen, die in der /VIAENET/-Umgebung definiert sind. Am Paket ist die Option `deinstall_allowed` gesetzt.

Verwandte Themen

- Einspielen des One Identity Manager Business Application Programing Interface auf Seite 18

Einrichten des Synchronisationsservers

Für die Einrichtung der Synchronisation mit einer SAP R/3-Umgebung muss ein Server zur Verfügung gestellt werden, auf dem die nachfolgend genannte Software installiert ist:

- Windows Betriebssystem

  Unterstützt werden die Versionen:

    - Windows Server 2008 R2 (nicht-Itanium 64-Bit) ab Service Pack 1
    - Windows Server 2012
    - Windows Server 2012 R2
    - Windows Server 2016
    - Windows Server 2019
- Microsoft .NET Framework Version 4.7.2 oder höher

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.
- Windows Installer
- SAP .Net Connector for .NET 4.0 on x64, mindestens Version 3.0.15.0
- One Identity Manager Service, Synchronization Editor, SAP R/3 Konnektor
    - Installieren Sie die One Identity Manager Komponenten mit dem Installationsassistenten.
        1. Wählen Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen**.
        2. Wählen Sie die Maschinenrolle **Server | Jobserver | SAP R/3**.

Weitere Anforderungen

- Folgende Dateien müssen entweder im Global Assemblies Cache (GAC) oder im Installationsverzeichnis des One Identity Manager vorhanden sein.
    - `libicudecnumber.dll`
    - `rscp4n.dll`
    - `sapnco.dll`
    - `sapnco_utils.dll`
- Folgende Dateien müssen entweder im Global Assemblies Cache (GAC) oder im Verzeichnis `C:\Windows\System32` oder im Installationsverzeichnis des One Identity Manager vorhanden sein.
    - `msvcp100.dll`
    - `msvcr100.dll`

Vom Synchronisationsserver werden alle Aktionen des One Identity Manager Service gegen die Zielsystemumgebung ausgeführt. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein.

HINWEIS: Wenn mehrere gleichartige Zielsystemumgebungen über den selben Synchronisationsserver synchronisiert werden sollen, ist es aus Performancegründen günstig, für jedes einzelne Zielsystem einen eigenen Jobserver einzurichten. Dadurch wird ein unnötiger Wechsel der Verbindungen zum Zielsystem vermieden, da stets nur gleichartige Aufträge von einem Jobserver zu verarbeiten sind (Nachnutzung bestehender Verbindungen).

Um den One Identity Manager Service zu installieren, nutzen Sie das Programm Server Installer. Das Programm führt folgende Schritte aus:

- Erstellen eines Jobservers.
- Festlegen der Maschinenrollen und Serverfunktionen für den Jobserver.
- Remote-Installation der One Identity Manager Service-Komponenten entsprechend der Maschinenrollen.
- Konfigurieren des One Identity Manager Service.
- Starten des One Identity Manager Service.

HINWEIS: Für die Generierung von Prozessen für die Jobserver werden der Provider, Verbindungsparameter und die Authentifizierungsdaten benötigt. Diese Informationen werden im Standardfall aus den Verbindungsdaten der Datenbank ermittelt. Arbeitet der Jobserver über einen Anwendungsserver müssen Sie zusätzliche Verbindungsinformationen im Designer konfigurieren. Ausführliche Informationen zum Einrichten des Jobservers finden Sie im *One Identity Manager Konfigurationshandbuch*.

HINWEIS: Das Programm führt eine Remote-Installation des One Identity Manager Service aus. Eine lokale Installation des Dienstes ist mit diesem Programm nicht möglich. Die Remote-Installation wird nur innerhalb einer Domäne oder in Domänen mit Vertrauensstellung unterstützt.

Für die Remote-Installation des One Identity Manager Service benötigen Sie eine administrative Arbeitsstation, auf der die One Identity Manager-Komponenten installiert sind. Ausführliche Informationen zur Installation einer Arbeitsstation finden Sie im *One Identity Manager Installationshandbuch*.

Um den One Identity Manager Service remote auf einem Server zu installieren und zu konfigurieren

1. Starten Sie das Programm Server Installer auf Ihrer administrativen Arbeitsstation.
2. Auf der Seite **Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.
3. Auf der Seite **Servereigenschaften** legen Sie fest, auf welchem Server der One Identity Manager Service installiert werden soll.
    a. Wählen Sie in der Auswahlliste **Server** einen Jobserver aus.

       - ODER -

       Um einen neuen Jobserver zur erstellen, klicken Sie **Hinzufügen**.
    b. Bearbeiten Sie folgende Informationen für den Jobserver.
        - **Server**: Bezeichnung des Jobservers.
        - **Queue**: Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue

angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.

- **Vollständiger Servername**: Vollständiger Servername gemäß DNS Syntax.

  Syntax:

  ```
  <Name des Servers>.<Vollqualifizierter Domänenname>
  ```

HINWEIS: Über die Option **Erweitert** können Sie weitere Eigenschaften für den Jobserver bearbeiten. Sie können die Eigenschaften auch zu einem späteren Zeitpunkt mit dem Designer bearbeiten.

4. Auf der Seite **Maschinenrollen** wählen Sie **SAP R/3**.
5. Auf der Seite **Serverfunktionen** wählen Sie **SAP R/3 Konnektor**.
6. Auf der Seite **Dienstkonfiguration** erfassen Sie die Verbindungsinformationen und prüfen Sie die Konfiguration des One Identity Manager Service.

   HINWEIS: Die initiale Konfiguration des Dienstes ist bereits vordefiniert. Sollte eine erweiterte Konfiguration erforderlich sein, können Sie diese auch zu einem späteren Zeitpunkt mit dem Designer durchführen. Ausführliche Informationen zur Konfiguration des Dienstes finden Sie im *One Identity Manager Konfigurationshandbuch*.

   - Für eine direkte Verbindung zu Datenbank:
     a. Wählen Sie **Prozessabholung | sqlprovider**
     b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     c. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
   - Für eine Verbindung zum Anwendungsserver:
     a. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
     b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     c. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.
     d. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
     e. Wählen Sie das Authentifizierungsmodul. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
7. Zur Konfiguration der Remote-Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** wählen Sie das Verzeichnis mit den Installationsdateien.

10. Auf der Seite **Datenbankschlüsseldatei auswählen** wählen die Datei mit dem privaten Schlüssel.

    HINWEIS: Diese Seite wird nur angezeigt, wenn die Datenbank verschlüsselt ist.

11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
    - **Computer**: Name oder IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
    - **Dienstkonto**: Angaben zum Benutzerkonto des One Identity Manager Service.
      - Um den Dienst unter dem Konto **NT AUTHORITY\SYSTEM** zu starten, aktivieren Sie die Option **Lokales Systemkonto**.
      - Um den Dienst unter einem anderen Konto zu starten, deaktivieren Sie die Option **Lokales Systemkonto** und erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung.
    - **Installationskonto**: Angaben zum administrativen Benutzerkonto für die Installation des Dienstes.
      - Um das Benutzerkonto des angemeldeten Benutzers zu verwenden, aktivieren Sie die Option **Angemeldeter Benutzer**.
      - Um ein anderes Benutzerkonto zu verwenden, deaktivieren Sie die Option **Angemeldeter Benutzer** und geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.
    - Um das Installationsverzeichnis, den Namen, den Anzeigenamen oder die Beschreibung für den One Identity Manager Service zu ändern, nutzen Sie die weiteren Optionen.
12. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.

    Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.
13. Auf der letzten Seite des Server Installer klicken Sie **Fertig**.

    HINWEIS: In einer Standardinstallation wird der Dienst mit der Bezeichnung **One Identity Manager Service** in der Dienstverwaltung des Servers eingetragen.

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines SAP Mandanten

Verwenden Sie den Synchronization Editor, um die Synchronisation zwischen One Identity Manager-Datenbank und SAP R/3-Umgebung einzurichten. Nachfolgend sind die Schritte für die initiale Einrichtung eines Synchronisationsprojektes beschrieben.

Nach der initialen Einrichtung können Sie innerhalb des Synchronisationsprojektes die Workflows anpassen und weitere Workflows konfigurieren. Nutzen Sie dazu den Workflow-Assistenten im Synchronization Editor. Der Synchronization Editor bietet zusätzlich verschiedene Konfigurationsmöglichkeiten für ein Synchronisationsprojekt an.

Für die Einrichtung des Synchronisationsprojektes halten Sie die folgenden Informationen bereit.

Tabelle 4: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
SAP R/3-Anwendungsserver	Name des Anwendungsserver, über den die RFC-Kommunikation stattfindet.
Systemnummer	Nummer des SAP Systems, mit dem sich der SAP R/3 Konnektor verbinden soll.
System-ID	System-ID dieses SAP Systems.
Mandant	Nummer des Mandanten, der synchronisiert werden soll. Wenn eine Zentrale Benutzerverwaltung (ZBV) synchronisiert werden soll, benötigen Sie die Mandantennummer des Zentralsystems.
Anmeldename und Kennwort	Name und Kennwort des Benutzerkontos, mit dem sich der SAP R/3 Konnektor am SAP R/3 System anmeldet. Stellen Sie ein Benutzerkonto mit ausreichenden Berechtigungen bereit. Wenn eine gesicherte Netzwerkverbindung hergestellt werden soll, benötigen Sie den SNC Namen des Benutzerkontos.
Loginsprache	Loginsprache für die Anmeldung des SAP R/3 Konnektors am SAP R/3-System.
Synchronisationsserver	Vom Synchronisationsserver werden alle Aktionen des One Identity Manager Service gegen die Zielsystemumgebung ausgeführt. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet. Installierte Komponenten: • SAP .Net Connector for .NET 4.0 on x64, mindestens Version 3.0.15.0 • One Identity Manager Service (gestartet) • Synchronization Editor • SAP R/3 Konnektor Der Synchronisationsserver muss im One Identity Manager

<table>
<tr><th>Angaben</th><th>Erläuterungen</th></tr>
<tr><td></td><td>als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften.

Tabelle 5: Zusätzliche Eigenschaften für den Jobserver
<table><tr><th>Eigenschaft</th><th>Wert</th></tr><tr><td>Serverfunktion</td><td>SAP R/3 Konnektor</td></tr><tr><td>Maschinenrolle</td><td>Server/Jobserver/SAP R/3</td></tr></table>
Weitere Informationen finden Sie unter Einrichten des Synchronisationsservers auf Seite 19.</td></tr>
<tr><td>Verbindungsdaten zur One Identity Manager-Datenbank</td><td>Datenbankserver
Datenbank
SQL Server Anmeldung und Kennwort
Angabe, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.</td></tr>
<tr><td>Remoteverbindungsserver</td><td>Um die Synchronisation mit einem Zielsystem zu konfigurieren, muss der One Identity Manager Daten aus dem Zielsystem auslesen. Dabei kommuniziert der One Identity Manager direkt mit dem Zielsystem. Mitunter ist der direkte Zugriff von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, nicht möglich, beispielsweise aufgrund der Firewall-Konfiguration oder weil die Arbeitsstation nicht die notwendigen Hard- oder Softwarevoraussetzungen erfüllt. Wenn der direkte Zugriff von der Arbeitsstation nicht möglich ist, kann eine Remoteverbindung eingerichtet werden.

Der Remoteverbindungsserver und die Arbeitsstation müssen in der selben Active Directory Domäne stehen.

Konfiguration des Remoteverbindungsservers:
One Identity Manager Service ist gestartet
RemoteConnectPlugin ist installiert
SAP R/3 Konnektor ist installiert
Der Remoteverbindungsserver muss im One Identity</td></tr>
</table>

Angaben	Erläuterungen
	Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt. TIPP: Der Remoteverbindungsserver benötigt dieselbe Konfiguration (bezüglich der installierten Software sowie der Berechtigungen des Benutzerkontos) wie der Synchronisationsserver. Nutzen Sie den Synchronisationsserver gleichzeitig als Remoteverbindungsserver, indem Sie lediglich das `RemoteConnectPlugin` zusätzlich installieren. Ausführliche Informationen zum Herstellen einer Remoteverbindung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Je nach Konfiguration des SAP R/3-Systems können zusätzliche Informationen für die Einrichtung des Synchronisationsprojekts benötigt werden.

Tabelle 6: Zusätzliche Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
SAP R/3-Router	Name des Routers, der dem SAP R/3 Konnektor einen Netzwerkport zur Kommunikation mit dem Anwendungsserver bereitstellt.
SAP R/3-Message-Server	Name des Message-Servers, mit dem der SAP R/3 Konnektor beim Login kommuniziert.
Logongruppe	Name der Logongruppe, bei der sich der SAP R/3 Konnektor anmeldet, wenn die Kommunikation innerhalb der SAP R/3-Umgebung über einen Message-Server läuft.
SNC Hostname	SNC Name des Hosts, zu dem die gesicherte Netzwerkverbindung hergestellt werden soll.
SNC Name	SNC Name des Benutzerkontos, mit dem sich der SAP R/3 Konnektor am SAP R/3-System anmeldet, wenn eine gesicherte Netzwerkverbindung hergestellt werden soll. Der SNC Name muss in der gleichen Syntax angegeben werden, wie er am Benutzerkonto in der SAP R/3-Umgebung hinterlegt ist.
SNC Client API	API, die die SNC Verschlüsselung enthält. Geben Sie den Dateinamen und Pfad auf dem Synchronisationsserver an. Wenn die Datei im Standardsuchpfad des Betriebssystems liegt, genügt der Dateiname. Wenn eine Verschlüsselung des Betriebssystems genutzt wurde, befindet sich die Datei im Betriebssystemverzeichnis und wird über den Standardsuchpfad gefunden. Wenn zur Verschlüsselung ein Drittanbieterprodukt genutzt wurde, wird die Datei nur dann gefunden, wenn das Installationsverzeichnis dieses Produkts zum Standardsuchpfad (PATH-Variable) hinzugefügt wurde.

HINWEIS: Der folgende Ablauf beschreibt die Einrichtung eines Synchronisationsprojekts, wenn der Synchronization Editor

- im Standardmodus ausgeführt wird und
- aus dem Launchpad gestartet wird.

Wenn der Projektassistent im Expertenmodus ausgeführt wird oder direkt aus dem Synchronization Editor gestartet wird, können zusätzliche Konfigurationseinstellungen vorgenommen werden. Folgen Sie in diesen Schritten den Anweisungen des Projektassistenten.

Um ein initiales Synchronisationsprojekt für einen SAP Mandanten einzurichten

1. Starten Sie das Launchpadund melden Sie sich an der One Identity Manager-Datenbank an.

   HINWEIS: Wenn die Synchronisation über einen Anwendungsserver ausgeführt werden soll, stellen Sie die Datenbankverbindung über den Anwendungsserver her.

2. Wählen Sie den Eintrag **Zielsystemtyp SAP R/3** und klicken Sie **Starten**.

   Der Projektassistent des Synchronization Editors wird gestartet.

3. Auf der Seite **Systemzugriff** legen Sie fest, wie der One Identity Manager auf das Zielsystem zugreifen kann.
   - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, möglich, nehmen Sie keine Einstellungen vor.
   - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, nicht möglich, können Sie eine Remoteverbindung herstellen.

     Aktivieren Sie die Option **Verbindung über einen Remoteverbindungsserver herstellen** und wählen Sie unter **Jobserver** den Server, über den die Verbindung hergestellt werden soll.

4. Auf der Seite **Verbindungstyp** wählen Sie den Verbindungstyp.

   Tabelle 7: Verbindungstypen

Eigenschaft	Beschreibung
SAP R/3-Anwendungsserver oder SAP R/3-Router	Angabe, ob die Verbindung über einen Anwendungsserver oder Router aufgebaut werden soll.
SAP R/3-Message-Server	Angabe, ob die Verbindung über einen Message-Server aufgebaut werden soll.

   - Auf der Seite **Verbindungsdaten** erfassen Sie die Verbindungsdaten für den Verbindungstyp "SAP R/3-Anwendungsserver oder SAP R/3-Router".

Tabelle 8: Systemverbindung

Eigenschaft	Beschreibung
SAP R/3-Host oder Router	Name des Anwendungsservers oder Routers, über den der SAP R/3 Konnektor kommuniziert.
Systemnummer	Nummer des SAP Systems.
System-ID	System-ID des SAP Systems. Sie wird in den One Identity Manager-Werkzeugen als Anzeigename verwendet.

- Auf der Seite **Message-Server** erfassen Sie die Verbindungsdaten für den Verbindungstyp "SAP R/3-Message-Server".

Tabelle 9: Systemverbindung

Eigenschaft	Beschreibung
SAP R/3-Message-Server	Name des Message-Servers, über den die Verbindung aufgebaut werden soll.
Logongruppe	Name der Logongruppe, bei der sich der SAP R/3 Konnektor anmeldet.
SAP R/3-Router	Name des Routers, wenn der SAP R/3 Konnektor über einen Router kommuniziert.
Systemnummer	Nummer des SAP Systems.
System-ID	System-ID des SAP Systems. Sie wird in den One Identity Manager-Werkzeugen als Anzeigename verwendet.

5. Auf der Seite **Gesicherte Verbindung** erfassen Sie die Netzwerkeinstellungen.

Tabelle 10: Netzwerkeinstellungen

Eigenschaft	Beschreibung
Program ID	Bezeichnung der Verbindung, die der SAP R/3 Konnektor mit dem SAP R/3-System aufbaut.
SNC Login	Angabe, ob zur Anmeldung des SAP R/3 Konnektors am SAP R/3-System der SNC Name des Benutzerkontos verwendet werden soll.

6. Wenn Sie auf der Seite **Gesicherte Verbindung** die Option **SNC Login** aktiviert haben, wird die Seite **SNC Verbindungskonfiguration** geöffnet. Erfassen Sie die Daten, die zur Anmeldung am Zielsystem über eine gesicherte Netzwerkverbindung benötigt werden.

Tabelle 11: SNC Systemverbindung

Eigenschaft	Beschreibung
Mandant	Nummer des Mandanten, der synchronisiert werden soll. Wenn eine Zentrale Benutzerverwaltung synchronisiert werden soll, geben Sie die Mandantennummer des Zentralsystems an.
SNC Hostname	SNC Name des Hosts, zu dem die gesicherte Netzwerk-verbindung hergestellt werden soll.
SNC Name	SNC Name des Benutzerkontos, mit dem sich der SAP R/3 Konnektor am SAP R/3-System anmeldet.
SNC Client API	API, welche die SNC Verschlüsselung enthält.
Authentifizierung	Wählen Sie die Sicherheitsstufe für die Anmeldung am SAP R/3-Systems aus.
Integritätsschutz	
Verschlüsselung	
Höchste verfügb. Stufe	
SNC Login mit Benutzername und Kennwort	Gibt an, ob beim SNC Login Benutzername und Kennwort explizit angegeben werden sollen. Wenn die Option deaktiviert ist, wird Single Sign-on zur Anmeldung genutzt.
Loginsprache	Loginsprache für die Anmeldung des SAP R/3 Konnektors am SAP R/3-System. Die gewählte Sprache entscheidet über die Sprache der Beschreibungstexte für alle SAP-Objekte dieses Mandanten. Wenn Sie hier „EN" wählen, werden alle Texte von SAP Gruppen, Rollen, Profilen und Startmenüs in englischer Sprache synchronisiert.

7. Auf der Seite **Anmeldedaten** erfassen Sie die Daten, die zur Anmeldung am Zielsystem benötigt werden.

Tabelle 12: Anmeldedaten

Eigenschaft	Beschreibung
Mandant	Nummer des Mandanten, der synchronisiert werden soll. Wenn eine Zentrale Benutzerverwaltung synchronisiert werden soll, geben Sie die Mandantennummer des Zentralsystems an.
Anmeldename	Name des Benutzerkontos, mit dem sich der SAP R/3 Konnektor am SAP R/3-System anmeldet. Wenn Sie auf der Seite **Gesicherte Verbindung** die Option **SNC Login** aktiviert

Eigenschaft	Beschreibung
	haben, geben Sie den SCN Namen dieses Benutzerkontos an.
Anmeldekennwort	Kennwort des Benutzerkontos, mit dem sich der SAP R/3 Konnektor am SAP R/3-System anmeldet.
Loginsprache	Loginsprache für die Anmeldung des SAP R/3 Konnektors am SAP R/3-System. Die gewählte Sprache entscheidet über die Sprache der Beschreibungstexte für alle SAP-Objekte dieses Mandanten. Wenn Sie hier „EN" wählen, werden alle Texte von SAP Gruppen, Rollen, Profilen und Startmenüs in englischer Sprache synchronisiert.

8. Auf der Seite **Zusätzliche Einstellungen** liefern Sie zusätzliche Informationen zur Synchronisation von Objekten und Eigenschaften. Sie können die Verbindungseinstellungen überprüfen.
   - Im Bereich **Zentrale Benutzerverwaltung (ZBV)** geben Sie an, ob die Verbindung zu einem Zentralsystem einer Zentralen Benutzerverwaltung aufgebaut werden soll. Aktivieren Sie in diesem Fall **Zentralsystem einer ZBV**.
   - Im Bereich **Verbindungseinstellungen prüfen** können Sie die erfassten Verbindungsdaten überprüfen. Klicken Sie **Jetzt prüfen**.

     Es wird versucht eine Verbindung zum Anwendungsserver aufzubauen. Wenn die Option **Zentralsystem einer ZBV** aktiviert ist, wird getestet, ob der angegebene Mandant das Zentralsystem einer ZBV ist.

     HINWEIS: Es wird nicht geprüft, ob das mitgelieferte BAPI eingespielt ist.
   - Um den Systemverbindungsassistenten zu beenden und zum Projektassistenten zurückzukehren, klicken Sie **Fertig**.
9. Auf der Seite **SAP HCM Einstellungen** klicken Sie **Weiter**.

   Diese Seite wird nur für die Synchronisation zusätzlicher Personalplanungsdaten im Modul SAP R/3 Strukturelle Profile Add-on benötigt.
10. Auf der Seite **SAP Konnektorschema** klicken Sie **Weiter**.

    TIPP: Auf dieser Seite können Sie eine Datei angeben, die zusätzliche Schematypen bereitstellt. Mit diesen Schematypen wird das Konnektorschema unternehmensspezifisch erweitert. Sie können diese Informationen auch nach dem Speichern des Synchronisationsprojekts erfassen. Weitere Informationen finden Sie unter Weitere Schematypen anlegen auf Seite 43.
11. Auf der Seite **One Identity Manager Verbindung** überprüfen Sie die Verbindungsdaten zur One Identity Manager-Datenbank. Die Daten werden aus der verbundenen Datenbank geladen. Geben Sie das Kennwort erneut ein.

    HINWEIS: Wenn Sie mit einer unverschlüsselten One Identity Manager-Datenbank arbeiten und noch kein Synchronisationsprojekt in der Datenbank gespeichert ist, erfassen Sie alle Verbindungsdaten neu. Wenn bereits ein Synchronisationsprojekt gespeichert ist, wird diese Seite nicht angezeigt.

12. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.
13. Auf der Seite **Projektvorlage auswählen** wählen Sie eine Projektvorlage, mit der die Synchronisationskonfiguration erstellt werden soll.

Tabelle 13: Standardprojektvorlagen

Projektvorlage	Beschreibung
SAP R/3 (untergeordnetes ZBV System)	Verwenden Sie diese Projektvorlage für die initiale Einrichtung des Synchronisationsprojektes für die Tochtersysteme einer ZBV, die zu einem anderen SAP System gehören als das Zentralsystem.
SAP R/3 Synchronisation (Basisadministration)	Verwenden Sie diese Projektvorlage für die initiale Einrichtung des Synchronisationsprojektes für einzelne Mandanten oder das Zentralsystem einer ZBV.

HINWEIS: Eine Standardprojektvorlage sorgt dafür, dass alle benötigten Informationen im One Identity Manager angelegt werden. Dazu gehören beispielsweise die Mappings, Workflows und das Basisobjekt der Synchronisation. Wenn Sie keine Standardprojektvorlage verwenden, müssen Sie das Basisobjekt der Synchronisation selbst im One Identity Manager bekannt geben. Verwenden Sie eine Standardprojektvorlage für die initiale Einrichtung des Synchronisationsprojektes. Für kundenspezifische Implementierungen können Sie das Synchronisationsprojekt mit dem Synchronization Editor erweitern.

14. Auf der Seite **Zielsystemzugriff einschränken** legen Sie fest, wie der Systemzugriff erfolgen soll. Zur Auswahl stehen:

Tabelle 14: Zielsystemzugriff festlegen

Option	Bedeutung
Das Zielsystem soll nur eingelesen werden.	Angabe, ob nur ein Synchronisationsworkflow zum initialen Einlesen des Zielsystems in die One Identity Manager-Datenbank eingerichtet werden soll. Der Synchronisationsworkflow zeigt folgende Besonderheiten: • Die Synchronisationsrichtung ist **In den One Identity Manager**. • In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung **In den One Identity Manager** definiert.
Es sollen auch	Angabe, ob zusätzlich zum Synchronisationsworkflow

Option	Bedeutung
Änderungen im Zielsystem durchgeführt werden.	zum initialen Einlesen des Zielsystems ein Provisionierungsworkflow eingerichtet werden soll. Der Provisionierungsworkflow zeigt folgende Besonderheiten: • Die Synchronisationsrichtung ist **In das Zielsystem**. • In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung **In das Zielsystem** definiert. • Synchronisationsschritte werden nur für solche Schemaklassen erstellt, deren Schematypen schreibbar sind.

Diese Seite wird nur angezeigt, wenn die Projektvorlage **SAP® R/3® Synchronisation (Basisadministration)** ausgewählt wurde. Wenn die Projektvorlage **SAP® R/3® (untergeordnetes ZBV System)** ausgewählt wurde, wird automatisch die Option **Das Zielsystem soll nur eingelesen werden.** aktiviert.

15. Auf der Seite **Synchronisationsserver** wählen Sie den Synchronisationsserver, der die Synchronisation ausführen soll.

    Wenn der Synchronisationsserver noch nicht als Jobserver in der One Identity Manager-Datenbank bekannt gegeben wurde, können Sie einen neuen Jobserver anlegen.

    a. Klicken Sie , um einen neuen Jobserver anzulegen.

    b. Erfassen Sie die Bezeichnung des Jobservers und den vollständigen Servernamen gemäß DNS-Syntax.

    c. Klicken Sie **OK**.

    Der Synchronisationsserver wird als Jobserver für das Zielsystem in der One Identity Manager-Datenbank bekannt gegeben.

    HINWEIS: Stellen Sie nach dem Speichern des Synchronisationsprojekts sicher, dass dieser Server als Synchronisationsserver eingerichtet ist.

16. Um den Projektassistenten zu beenden, klicken Sie **Fertig**.

    Es wird ein Standardzeitplan für regelmäßige Synchronisationen erstellt und zugeordnet. Aktivieren Sie den Zeitplan für die regelmäßige Synchronisation.

    Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

    HINWEIS:Beim Aktivieren wird eine Konsistenzprüfung durchgeführt. Wenn dabei Fehler auftreten, erscheint eine Meldung. Sie können entscheiden, ob das Synchronisationsprojekt dennoch aktiviert werden soll.

Bevor Sie das Synchronisationsprojekt nutzen, prüfen Sie die Fehler. In der Ansicht **Allgemein** auf der Startseite des Synchronization Editor klicken Sie dafür **Projekt prüfen**.

HINWEIS: Wenn das Synchronisationsprojekt nicht sofort aktiviert werden soll, deaktivieren Sie die Option **Synchronisationsprojekt speichern und sofort aktivieren**. In diesem Fall speichern Sie das Synchronisationsprojekt manuell vor dem Beenden des Synchronization Editor.

Deaktivieren Sie diese Option, wenn Sie eigene Schematypen in diesem Synchronisationsprojekt anlegen möchten.

HINWEIS: Die Verbindungsdaten zum Zielsystem werden in einem Variablenset gespeichert und können bei Bedarf im Synchronization Editor in der Kategorie **Konfiguration | Variablen** angepasst werden.

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Um das Synchronisationsprotokoll für die Zielsystemverbindung zu konfigurieren, wählen Sie die Kategorie **Konfiguration | Zielsystem**.
3. Um das Synchronisationsprotokoll für die Datenbankverbindung zu konfigurieren, wählen Sie die Kategorie **Konfiguration | One Identity Manager Verbindung**.
4. Wählen Sie den Bereich **Allgemein** und klicken Sie **Konfigurieren**.
5. Wählen Sie den Bereich **Synchronisationsprotokoll** und aktivieren Sie **Synchronisationsprotokoll erstellen**.
6. Aktivieren Sie die zu protokollierenden Daten.

   HINWEIS: Einige Inhalte erzeugen besonders viele Protokolldaten. Das Synchronisationsprotokoll soll nur die für Fehleranalysen und weitere Auswertungen notwendigen Daten enthalten.
7. Klicken Sie **OK**.

Um regelmäßige Synchronisationen auszuführen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Konfiguration | Startkonfigurationen**.
3. Wählen Sie in der Dokumentenansicht eine Startkonfiguration aus und klicken Sie **Zeitplan bearbeiten**.
4. Bearbeiten Sie die Eigenschaften des Zeitplans.
5. Um den Zeitplan zu aktivieren, klicken Sie **Aktiviert**.
6. Klicken Sie **OK**.

Um die initiale Synchronisation manuell zu starten

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Konfiguration | Startkonfigurationen**.
3. Wählen Sie in der Dokumentenansicht eine Startkonfiguration und klicken Sie

Ausführen.

4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

HINWEIS:

Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Personen erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für den Mandanten bekannt, werden die Benutzerkonten mit den Personen verbunden. Es wird jedoch noch keine Kontendefinition zugewiesen. Die Benutzerkonten sind somit im Zustand **Linked** (verbunden).

Um die Benutzerkonten über Kontendefinitionen zu verwalten, weisen Sie diesen Benutzerkonten eine Kontendefinition und einen Automatisierungsgrad zu.

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie dem Mandanten die Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand **Linked** (verbunden) die Kontendefinition zu. Es wird der Standardautomatisierungsgrad der Kontendefinition für das Benutzerkonto übernommen.
    a. Wählen Sie im Manager die Kategorie **SAP R/3 | Benutzerkonten | Verbunden aber nicht konfiguriert | <Mandant>**.
    b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.
    c. Wählen Sie in der Auswahlliste **Kontendefinition** die Kontendefinition.
    d. Wählen Sie die Benutzerkonten, die die Kontendefinition erhalten sollen.
    e. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation

Verwandte Themen

- Einrichten des Synchronisationsservers auf Seite 19
- Benutzer und Berechtigungen für die Synchronisation mit einer SAP R/3-Umgebung auf Seite 15
- Synchronisationsergebnisse anzeigen auf Seite 38
- Anpassen einer Synchronisationskonfiguration auf Seite 39
- Beschleunigung der Synchronisation durch Revisionsfilterung auf Seite 54
- Standardprojektvorlagen für die Synchronisation einer SAP R/3-Umgebung auf Seite 227
- Einrichten von Kontendefinitionen auf Seite 66

- Automatische Zuordnung von Personen zu SAP Benutzerkonten auf Seite 156
- Weitere Schematypen anlegen auf Seite 43

Besonderheiten bei der Synchronisation mit dem Zentralsystem einer ZBV

HINWEIS:

- Es werden nur die Rollen und Profile der Tochtersysteme im One Identity Manager abgebildet, die der Anmeldesprache des administrativen Benutzerkontos für die Synchronisation entsprechen!
- Pflegen Sie alle Rollen und Profile der Tochtersysteme im Zielsystem in der Sprache, die im Synchronisationsprojekt für das Zentralsystem in der Systemverbindung als Loginsprache hinterlegt ist.

Soll eine Zentrale Benutzerverwaltung an den One Identity Manager angeschlossen werden, ist eine regelmäßige Synchronisation nur mit dem Zentralsystem erforderlich. Die Synchronisationskonfiguration wird für den Mandanten erstellt, der als Zentralsystem gekennzeichnet ist. Bei der Synchronisation wird das Application Link Enabling (ALE)-Verteilungsmodell der ZBV ausgelesen und versucht, alle Mandanten, die als Tochtersystem konfiguriert sind, dem Zentralsystem im One Identity Manager zuzuordnen. Dabei werden alle Mandanten, die sich im selben SAP System wie das Zentralsystem befinden, automatisch im One Identity Manager angelegt und dem Zentralsystem zugeordnet (Eingabefeld **Zentralsystem der ZBV**). Alle Mandanten, die sich in einem anderen SAP System befinden, müssen zu diesem Zeitpunkt bereits im One Identity Manager existieren.

Wenn im Zielsystem ein Textabgleich der Rollen und Profile zwischen Tochtersystemen und Zentralsystem durchgeführt wurde, werden die Rollen und Profile der Tochtersysteme bei der Synchronisation berücksichtigt. Diese Rollen und Profile werden im One Identity Manager den Mandanten zugeordnet, aus denen sie ursprünglich stammen.

Beim Textabgleich der Rollen und Profile zwischen Tochtersystem und Zentralsystem im Zielsystem werden die Rollen und Profile sprachabhängig in der Tabelle USRSYSACTT gespeichert. Bei der Synchronisation mit dem One Identity Manager werden nur die Rollen und Profile aus der Tabelle USRSYSACTT ausgelesen, die der Anmeldesprache des administrativen Benutzerkontos für die Synchronisation entsprechen. Sind einzelne Rollen oder Profile nicht in dieser Sprache gepflegt, werden sie nicht in den One Identity Manager übernommen. Damit alle Rollen und Profile aus den Tochtersystemen im One Identity Manager abgebildet werden, müssen sie alle im Zielsystem in der Sprache gepflegt werden, die als Loginsprache am Zentralsystem hinterlegt ist.

Um ein initiales Synchronisationsprojekt für eine Zentrale Benutzerverwaltung einzurichten

1. Erstellen Sie Synchronisationsprojekte für die Tochtersysteme, die sich nicht im selben SAP System befinden, wie das Zentralsystem.

Gehen Sie wie in Abschnitt Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines SAP Mandanten auf Seite 23 beschrieben vor. Es gelten folgende Besonderheiten:

a. Wählen Sie im Projektassistenten auf der Seite **Projektvorlage auswählen** die Projektvorlage "SAP R/3 (untergeordnetes ZBV System)".

b. Die Seite **Zielsystemzugriff einschränken** wird nicht angezeigt. Das Zielsystem soll nur eingelesen werden.

c. Starten Sie die Synchronisation manuell, um die benötigten Daten einzulesen.

   Es werden alle Mandanten aus dem ausgewählten System und deren Lizenzinformationen eingelesen.

   > HINWEIS: Führen Sie keine zeitgesteuerten Synchronisationen aus. Eine erneute Synchronisation ist nur erforderlich, wenn die aktiven Preislisten für die Lizenzberechnung im Zielsystem geändert wurden.

2. Wiederholen Sie den Schritt 1 für alle Tochtersysteme, die sich in weiteren untergeordneten SAP Systemen befinden.
3. Erstellen Sie ein Synchronisationsprojekt für das Zentralsystem.

   Gehen Sie wie in Abschnitt Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines SAP Mandanten auf Seite 23 beschrieben vor. Es gelten folgende Besonderheiten:

   a. Aktivieren Sie auf der Seite **Zusätzliche Einstellungen** die Option **Zentralsystem einer ZBV**.

   b. Wählen Sie auf der Seite **Projektvorlage auswählen** die Projektvorlage "SAP R/3 Synchronisation (Basisadministration)".

   c. Konfigurieren Sie die zeitgesteuerte Synchronisation.
4. Nachdem alle Tochtersysteme aus untergeordneten SAP Systemen in die One Identity Manager-Datenbank eingelesen wurden, starten Sie die Synchronisation des Zentralsystems.

Verwandte Themen

- Allgemeine Stammdaten eines SAP Mandanten auf Seite 122
- Tochtersystem von der Synchronisation ausschließen auf Seite 36

Tochtersystem von der Synchronisation ausschließen

Bestimmte administrative Aufgaben in der SAP R/3-Umgebung erfordern, dass Tochtersysteme zeitweilig aus der Zentralen Benutzerverwaltung ausgeschlossen werden. Werden diese Tochtersysteme während dieser Zeit synchronisiert, dann werden, abhängig von der Konfiguration der Synchronisation, die SAP Rollen und SAP Profile des ausgeschlossenen Tochtersystems in der One Identity Manager-Datenbank als ausstehend

gekennzeichnet oder gelöscht. Um das zu verhindern, entfernen Sie das Tochtersystem aus dem Synchronisationsscope.

Durch das Löschen des ALE Modellnamens am Mandanten werden die SAP Rollen und Profile des Tochtersystems aus dem Scope der Synchronisation entfernt. Die Eigenschaften des Mandanten werden jedoch synchronisiert. Damit der ALE Modellname dabei nicht wieder eingefügt wird, deaktivieren Sie die Regel für das Mapping dieser Schemaeigenschaft.

Um ein Tochtersystem von der Synchronisation auszuschließen

1. Wählen Sie die Kategorie **SAP R/3 | Mandanten**.
2. Wählen Sie in der Ergebnisliste das Tochtersystem. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Löschen Sie den Eintrag im Eingabefeld **ALE Modellname**.
4. Speichern Sie die Änderungen.
5. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
6. Wählen Sie die Kategorie **Workflows**.
7. Wählen Sie in der Navigationsansicht den Workflow, der für die Synchronisation des Zentralsystems genutzt wird.
8. Doppelklicken Sie in der Workflowansicht auf den Synchronisationsschritt "mandant".
9. Wählen Sie den Tabreiter **Regelfilter**.
10. Aktivieren Sie im Bereich **Auszuschließende Regeln** die Property-Mapping-Regel "ALEModelName_ALEModelName".
11. Klicken Sie **OK**.
12. Speichern Sie die Änderungen.

HINWEIS: Abhängig von den Einstellungen im Synchronisationsprotokoll werden nicht erfolgreiche Datenbankoperationen für Zuweisungen von SAP Rollen und Profilen zu Benutzerkonten, die aus dem zeitweilig ausgeschlossenen Tochtersystem stammen, protokolliert. Diese Meldungen können ignoriert werden. Sobald das Tochtersystem wieder verfügbar ist, werden diese Mitgliedschaften korrekt bearbeitet.

Sobald das Tochtersystem wieder Bestandteil der Zentralen Benutzerverwaltung ist, muss auch die Synchronisation der SAP Rollen und Profile wieder aktiviert werden.

Um ein Tochtersystem wieder in die Synchronisation einzubeziehen

1. Wählen Sie die Kategorie **SAP R/3 | Mandanten**.
2. Wählen Sie in der Ergebnisliste das Tochtersystem. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Erfassen Sie im Eingabefeld **ALE Modellname** den ALE Modellnamen des Zentralsystems der ZBV.

   Das Tochtersystem wird nur synchronisiert, wenn am Zentralsystem und am Tochtersystem derselbe ALE Modellname angegeben ist.
4. Speichern Sie die Änderungen.

5. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
6. Wählen Sie die Kategorie **Workflows**.
7. Wählen Sie in der Navigationsansicht den Workflow, der für die Synchronisation des Zentralsystems genutzt wird (standardmäßig "Initial Synchronization").
8. Doppelklicken Sie in der Workflowansicht auf den Synchronisationsschritt "mandant".
9. Wählen Sie den Tabreiter **Regelfilter**.
10. Deaktivieren Sie im Bereich **Auszuschließende Regeln** die Property-Mapping-Regel "ALEModelName_ALEModelName".
11. Klicken Sie **OK**.
12. Speichern Sie die Änderungen.

Ausführliche Informationen zur Bearbeitung von Synchronisationsschritten finden Sie im One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation.

Verwandte Themen

- Allgemeine Stammdaten eines SAP Mandanten auf Seite 122

Synchronisationsergebnisse anzeigen

Die Ergebnisse der Synchronisation werden im Synchronisationsprotokoll zusammengefasst. Der Umfang des Synchronisationsprotokolls kann für jede Systemverbindung separat festgelegt werden. Der One Identity Manager stellt verschiedene Berichte bereit, in denen die Synchronisationsergebnisse nach verschiedenen Kriterien aufbereitet sind.

Um das Protokoll einer Synchronisation anzuzeigen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Protokolle**.
3. Klicken Sie in der Symbolleiste der Navigationsansicht ▶.

   In der Navigationsansicht werden die Protokolle aller abgeschlossenen Synchronisationsläufe angezeigt.
4. Wählen Sie per Maus-Doppelklick das Protokoll, das angezeigt werden soll.

   Die Auswertung der Synchronisation wird als Bericht angezeigt. Sie können diesen Bericht speichern.

Um das Protokoll einer Provisionierung anzuzeigen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Protokolle**.
3. Klicken Sie in der Symbolleiste der Navigationsansicht

.

In der Navigationsansicht werden die Protokolle aller abgeschlossenen Provisionierungsprozesse angezeigt.

4. Wählen Sie per Maus-Doppelklick das Protokoll, das angezeigt werden soll.

   Die Auswertung der Provisionierung wird als Bericht angezeigt. Sie können diesen Bericht speichern.

Die Protokolle sind in der Navigationsansicht farblich gekennzeichnet. Die Kennzeichnung gibt den Ausführungsstatus der Synchronisation/Provisionierung wieder.

TIPP: Die Protokolle werden auch im Manager unter der Kategorie **<Zielsystemtyp> | Synchronisationsprotokolle** angezeigt.

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

- Aktivieren Sie im Designer den Konfigurationsparameter **DPR | Journal | LifeTime** und tragen Sie die maximale Aufbewahrungszeit ein.

Anpassen einer Synchronisationskonfiguration

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation eines SAP Mandanten eingerichtet. Mit diesem Synchronisationsprojekt können Sie SAP Objekte in die One Identity Manager-Datenbank einlesen. Wenn Sie Benutzerkonten und ihre Berechtigungen mit dem One Identity Manager verwalten, werden Änderungen in die SAP-Umgebung provisioniert.

Um die Datenbank und die SAP R/3-Umgebung regelmäßig abzugleichen und Änderungen zu synchronisieren, passen Sie die Synchronisationskonfiguration an.

- Um bei der Synchronisation den One Identity Manager als Mastersystem zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um festzulegen, welche SAP Objekte und Datenbankobjekte bei der Synchronisation behandelt werden, bearbeiten Sie den Scope der Zielsystemverbindung und der One Identity Manager-Datenbankverbindung. Um Dateninkonsistenzen zu vermeiden, definieren Sie in beiden Systemen den gleichen Scope. Ist kein Scope definiert, werden alle Objekte synchronisiert.
- Um allgemeingültige Synchronisationskonfigurationen zu erstellen, die erst beim Start der Synchronisation die notwendigen Informationen über die zu synchronisierenden Objekte erhalten, können Variablen eingesetzt werden. Variablen können beispielsweise in den Basisobjekten, den Schemaklassen oder den Verarbeitungsmethoden eingesetzt werden.

- Mit Hilfe von Variablen kann ein Synchronisationsprojekt für die Synchronisation verschiedener Mandanten eingerichtet werden. Hinterlegen Sie die Verbindungsparameter zur Anmeldung an den Mandanten als Variablen.
- Wenn sich das One Identity Manager Schema oder das Zielsystemschema geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.
- Um Daten zu synchronisieren, für die keine Schematypen im Konnektorschema angelegt sind, legen Sie eigene Schematypen an.

WICHTIG: Solange eine Synchronisation ausgeführt wird, sollte keine weitere Synchronisation für dasselbe Zielsystem gestartet werden. Das gilt insbesondere, wenn dieselben Synchronisationsobjekte verarbeitet werden.

- Wenn eine weitere Synchronisation mit derselben Startkonfiguration gestartet wird, wird dieser Prozess gestoppt und erhält den Ausführungsstatus **Frozen**. Es wird eine Fehlermeldung in die Protokolldatei des One Identity Manager Service geschrieben.
    - Stellen Sie sicher, dass Startkonfigurationen, die in Startfolgen verwendet werden, nicht gleichzeitig einzeln gestartet werden. Weisen Sie den Startfolgen und Startkonfigurationen unterschiedliche Zeitpläne zu.
- Wenn eine weitere Synchronisation mit einer anderen Startkonfiguration gestartet wird, die dasselbe Zielsystem anspricht, kann das zu Synchronisationsfehlern oder Datenverlust führen. Legen Sie an den Startkonfigurationen fest, wie sich der One Identity Manager in diesem Fall verhalten soll.
    - Stellen Sie über den Zeitplan sicher, dass die Startkonfigurationen nacheinander ausgeführt werden.
    - Gruppieren Sie die Startkonfigurationen mit gleichem Startverhalten.

Ausführliche Informationen zum Konfigurieren einer Synchronisation finden Sie im One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation.

Detaillierte Informationen zum Thema

- Synchronisation in die SAP R/3-Umgebung konfigurieren auf Seite 40
- Synchronisation verschiedener Mandanten konfigurieren auf Seite 41
- Schema aktualisieren auf Seite 42
- Weitere Schematypen anlegen auf Seite 43

Synchronisation in die SAP R/3-Umgebung konfigurieren

Das Synchronisationsprojekt für die initiale Synchronisation stellt je einen Workflow zum initialen Einlesen der Zielsystemobjekte (Initial Synchronization) und für die Provisionierung von Objektänderungen aus der One Identity Manager-Datenbank in das

Zielsystem (Provisioning) bereit. Um bei der Synchronisation den One Identity Manager als Mastersystem zu nutzen, benötigen Sie zusätzlich einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.

Um eine Synchronisationskonfiguration für die Synchronisation in die SAP R/3-Umgebung zu erstellen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Prüfen Sie, ob die bestehenden Mappings für die Synchronisation in das Zielsystem genutzt werden können. Erstellen Sie bei Bedarf neue Mappings.
3. Erstellen Sie mit dem Workflowassistenten einen neuen Workflow.

   Es wird ein Workflow mit der Synchronisationsrichtung **In das Zielsystem** angelegt.
4. Erstellen Sie eine neue Startkonfiguration. Nutzen Sie dabei den neu angelegten Workflow.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

Verwandte Themen

- Synchronisation verschiedener Mandanten konfigurieren auf Seite 41

Synchronisation verschiedener Mandanten konfigurieren

Voraussetzungen

- Die Zielsystemschemas beider Mandanten sind identisch.
- Alle virtuellen Schemaeigenschaften, die im Mapping genutzt werden, müssen in den erweiterten Schemas beider Mandanten vorhanden sein.

Um ein Synchronisationsprojekt für die Synchronisation eines weiteren Mandaten anzupassen

1. Stellen Sie in dem weiteren Mandanten ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
3. Erstellen Sie für den weiteren Mandanten ein neues Basisobjekt. Verwenden Sie den Assistenten zur Anlage eines Basisobjektes.
   - Wählen Sie im Assistenten den SAP Konnektor und geben Sie die Verbindungsparameter bekannt. Die Verbindungsparameter werden in einem spezialisierten Variablenset gespeichert.

Es wird eine Startkonfiguration erstellt, die das neu angelegte Variablenset verwendet.

4. Passen Sie bei Bedarf weitere Komponenten der Synchronisationskonfiguration an.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

Verwandte Themen

- Synchronisation in die SAP R/3-Umgebung konfigurieren auf Seite 40

Schema aktualisieren

Während ein Synchronisationsprojekt bearbeitet wird, stehen alle Schemadaten (Schematypen und Schemaeigenschaften) des Zielsystemschemas und des One Identity Manager Schemas zur Verfügung. Für eine Synchronisationskonfiguration wird jedoch nur ein Teil dieser Daten benötigt. Wenn ein Synchronisationsprojekt fertig gestellt wird, werden die Schemas komprimiert, um die nicht benötigten Daten aus dem Synchronisationsprojekt zu entfernen. Dadurch kann das Laden des Synchronisationsprojekts beschleunigt werden. Die entfernten Schemadaten können zu einem späteren Zeitpunkt wieder in die Synchronisationskonfiguration aufgenommen werden.

Wenn sich das Zielsystemschema oder das One Identity Manager Schema geändert hat, müssen diese Änderungen ebenfalls in die Synchronisationskonfiguration aufgenommen werden. Anschließend können die Änderungen in das Mapping der Schemaeigenschaften eingearbeitet werden.

Um Schemadaten, die beim Komprimieren entfernt wurden, und Schemaänderungen in der Synchronisationskonfiguration berücksichtigen zu können, aktualisieren Sie das jeweilige Schema im Synchronisationsprojekt. Das kann erforderlich sein, wenn:

- ein Schema geändert wurde, durch:
  - Änderungen am Zielsystemschema
  - unternehmensspezifische Anpassungen des One Identity Manager Schemas
  - eine Update-Migration des One Identity Manager
- ein Schema im Synchronisationsprojekt komprimiert wurde, durch:
  - die Aktivierung des Synchronisationsprojekts
  - erstmaliges Speichern des Synchronisationsprojekts
  - Komprimieren eines Schemas

Um das Schema einer Systemverbindung zu aktualisieren

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Konfiguration | Zielsystem**.

- ODER -

Wählen Sie die Kategorie **Konfiguration | One Identity Manager Verbindung**.

3. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Die Schemadaten werden neu geladen.

Um ein Mapping zu bearbeiten

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Mappings**.
3. Wählen Sie in der Navigationsansicht das Mapping.

   Der Mappingeditor wird geöffnet. Ausführliche Informationen zum Bearbeiten von Mappings finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

HINWEIS: Wenn das Schema eines aktivierten Synchronisationsprojekts aktualisiert wird, wird das Synchronisationsprojekt deaktiviert. Damit Synchronisationen ausgeführt werden, aktivieren Sie das Synchronisationsprojekt erneut.

Weitere Schematypen anlegen

Wenn Sie Daten synchronisieren möchten, für die keine Schematypen im Konnektorschema angelegt sind, legen Sie eigene Schematypen an. Die eigenen Schematypen können Sie bereits beim Einrichten des initialen Synchronisationsprojekts mit dem Projektassistenten anlegen lassen. Sie können aber auch nach dem Speichern des Synchronisationsprojekts angelegt werden. Dieser Weg ist hier beschrieben.

Im Zielsystembrowser des Synchronization Editors können Sie sich einen Überblick verschaffen, welche Schematypen im Konnektorschema definiert sind.

WICHTIG: Im Zielsystembrowser werden sowohl genutzte, als auch ungenutzte Schematypen angezeigt. Wenn das Synchronisationsprojekt aktiviert wird, werden die ungenutzten Schematypen aus dem Schema gelöscht. Sie werden damit nicht mehr im Zielsystembrowser angezeigt.

Prüfen Sie die Liste der Schematypen, bevor Sie das Synchronisationsprojekt aktivieren.

Um den Zielsystembrowser zu starten

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Konfiguration | Zielsystem**.
3. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Durchsuchen...**.

   Der Zielsystembrowser wird geöffnet. In der Ansicht **Schematypen** sehen Sie im oberen Bereich alle Schematypen, die in diesem Synchronisationsprojekt genutzt werden. Der untere Bereich enthält die Liste der ungenutzten Schematypen.

Um das Konnektorschema mit eigenen Schematypen zu erweitern

1. Ermitteln Sie, welche Schematypen Sie benötigen.
2. Erstellen Sie eine Schemaerweiterungsdatei. Speichern Sie diese Datei und halten Sie den Dateinamen und den Ablagepfad bereit.

   Weitere Informationen finden Sie unter Schemaerweiterungsdatei erstellen auf Seite 45.
3. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
4. Wählen Sie die Kategorie **Konfiguration | Zielsystem**.
5. Klicken Sie **Verbindung bearbeiten**.

   Der Systemverbindungsassistent wird gestartet.
6. Prüfen Sie die erfassten Daten.
7. Auf der Seite **SAP Konnektorschema** erfassen Sie den Namen und den Pfad zur Schemaerweiterungsdatei.
   a. Um die Schemaerweiterungsdatei auf logische Fehler zu überprüfen, klicken Sie **Datei prüfen**.

      Alle definierten Schematypen werden aufgelistet.
   b. Klicken Sie **Weiter**.
8. Um den Systemverbindungsassistenten zu beenden, klicken Sie **Fertig**.
9. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
10. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

    Die Schemadaten, einschließlich der neuen Schematypen, werden geladen.
11. Öffnen Sie den Zielsystembrowser und prüfen Sie, ob die Schematypen angelegt wurden.

    Die Schematypen werden in der Liste der ungenutzten Schematypen angezeigt.
12. Wählen Sie die Kategorie **Mappings** und erstellen Sie Mappings für die neu angelegten Schematypen. Beachten Sie dabei, ob diese nur gelesen oder auch geschrieben werden können.

    Ausführliche Informationen zum Einrichten von Mappings und Schemaklassen finden Sie im*One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.
13. Wählen Sie die Kategorie **Workflows** und bearbeiten Sie die Workflows. Erstellen Sie zusätzliche Synchronisationsschritte für die neu angelegten Mappings. Beachten Sie dabei, ob die Schematypen nur gelesen oder auch geschrieben werden können.

    Ausführliche Informationen zum Erstellen von Synchronisationsschritten finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.
14. Speichern Sie die Änderungen.
15. Führen Sie eine Konsistenzprüfung durch.
16. Aktivieren Sie das Synchronisationsprojekt.

Schemaerweiterungsdatei erstellen

In der Schemaerweiterungsdatei werden alle Schematypen definiert, mit denen das Konnektorschema erweitert werden soll. Die Schemaerweiterungsdatei ist eine XML-Datei, die einen identischen Aufbau wie das Konnektorschema hat. Sie beschreibt die Definitionen für Tabellenabfragen und BAPI-Aufrufe für die neuen Schematypen. Wenn ein neuer Schematyp denselben Name hat, wie ein bereits vorhandener Schematyp, wird die Erweiterung ignoriert.

Die Datei gliedert sich in drei Hauptbereiche:

- Definitionsteil für Tabellen
- Definitionsteil für Funktionen
- Definitionsteil für Schematypen

Grundsätzlich müssen zuerst alle Tabellen und Funktionen, die zum Zugriff auf Daten für die zu definierenden Schematypen benötigt werden, deklariert werden. Anschließend können im Definitionsteil für Schematypen die neuen Schematypen definiert werden. Funktionen und Tabellen dürfen dabei in verschiedenen Schematypdefinitionen verwendet werden. Eine Schematypdefinition muss mindestens den Aufruf für eine Objektliste enthalten.

Struktur der Schemaerweiterungsdatei

```
<?xml version="1.0" encoding="utf-8" ?>
<SAP>
      <Tables>
      ...
      </Tables>
      <Functions>
      ...
      </Functions>
      <SAPExtendedSchematypes>
      ...
      </SAPExtendedSchematypes>
</SAP>
```

Vordefinierte Variablen

Im Definitionsteil für Tabellen und Funktionen können Variablen verwendet werden. Nutzbar sind alle Systemvariablen, die der SAP-Baustein `RFC_READ_TABLE` kennt.

Tabelle 15: Beispiele für Systemvariablen

Variable	Beschreibung
sy-langu	Aktuell gewählte Anmeldesprache.
sy–datum	Aktuelles Datum.
sy-mandant	Aktueller Mandant der Anmeldung.

Außerdem können Variablen genutzt werden, die der SAP R/3 Konnektor kennt, beispielsweise aus der Definition von Prozessparametern.

Tabelle 16: Vordefinierte Variablen des SAP R/3 Konnektors

Variable	Beschreibung
$Value$	Eingabeparameter des One Identity Manager Service-Aufrufs.
$Mandt$	Nummer des aktuellen Mandanten.
$Date$	Aktuelles Datum.

Detaillierte Informationen zum Thema

- Tabellen definieren auf Seite 46
- Funktionen definieren auf Seite 49
- Schematypen definieren auf Seite 50
- Beispiel für eine Schemaerweiterungsdatei auf Seite 234

Tabellen definieren

Im Definitionsteil für Tabellen (`Tables`) werden die Tabellen und Spalten selektiert, die zum Zugriff auf die Daten für die zu definierenden Schematypen benötigt werden. Der SAP R/3 Konnektor benötigt für jede Tabelle eine Definition zum Laden der schlanken Objektliste. Dafür definieren Sie genau die Spalten, die der SAP R/3 Konnektor bereits beim Laden der zu synchronisierenden Objekte benötigt. Beim Einzelobjektzugriff werden immer alle Spalten der Tabelle geladen.

Tabelle 17: Tabellendefinition

Attribut	Beschreibung
Definition	Symbolischer Name zur Verwendung der Definition.
TableName	Tabellenname in der SAP Datenbank.
Key	Schlüsselbegriffe zur Bildung eines definierten Namens. Die Angabe von mehreren Werten als kommagetrennte Liste ist möglich.

Attribut	Beschreibung
X500	Kürzel für die Schlüsselbegriffe im Attribut `Key`. Die Angabe von mehreren Werten als kommagetrennte Liste ist möglich.
SQL	Einschränkende Where-Klausel. HINWEIS: Es gibt einige Beschränkungen bei der Auswertung der SQL-Operatoren im SAP R/3-System. Für ein korrektes Ergebnis beachten Sie folgende Regeln: • Bei Vergleichsoperationen muss der Spaltenname vor dem Operator stehen, dahinter der Vergleichswert (Beispiel: `BEGDA LT sy-datum`). • Die Nutzung der Vergleichsoperatoren "<" und ">" verursacht Auswertungsfehler im XML. Stattdessen müssen die Operatoren `LT` und `GT` verwendet werden. Weitere Informationen finden Sie unter Zulässige Operatoren im SQL-Attribut auf Seite 48.
Distinct	Aufzählung der Spalten, über die insgesamt ein `Distinct`–Filter wirkt (als kommagetrennte Liste).
Load	Spalten, die zur Ladezeit der Objektliste bereits zu laden sind. Diese Spalten können beispielsweise zur Bildung des Anzeigenamens (`DisplayPattern`) des Schematyps, als Revisionszähler oder als Eingabeparameter in einer Funktion verwendet werden. Wenn die Objektliste aus einer Tabelle, aber die Einzelobjekte aus einer Funktion geladen werden sollen, müssen hier alle Spalten angegeben werden, die innerhalb des Synchronisationsprojekts im Mapping verwendet werden sollen. WICHTIG: Jede Spalte, die beim Laden der Objektliste zusätzlich geladen werden muss, erzeugt zusätzliche Last im One Identity Manager. Bei großen Datenmengen kann die Synchronisation dadurch deutlich langsamer werden. Geben Sie hier nur Spalten an, die für die weitere Verarbeitung der Objekte zwingend benötigt werden. Für den Einzelobjektzugriff werden keine Angaben benötigt.

Hinweise

- Es können mehrere Tabellendefinitionen mit verschiedenen symbolischen Namen, die sich auf dieselbe Tabelle in der SAP Datenbank beziehen, definiert werden.
- Schlüsselspalten werden immer geladen. Sie sollen daher nicht im Attribut `Load` angegeben werden.
- Das Attribut `Load` wirkt nur beim Laden der Objektliste. Beim Einzelobjektzugriff über eine Tabelle werden immer alle Spalten der Tabelle geladen.
- Als Operatoren in der Where-Klausel sind zulässig:

Tabelle 18: Zulässige Operatoren im SQL-Attribut

Operator	Funktion/Beispiel
EQ	=
NE	<>
GT	>
LT	<
GE	>=
LE	<=
BETWEEN	ENDDA BETWEEN '20090101' AND '20090131'

- Eine Tabellendefinition kann zusätzlich einen Mapping-Block enthalten. Dieser Block dient der Umsetzung von Parametern, die in Where-Klauseln verwendet werden sollen, aber in der Objektliste mit einem anderen Spaltennamen selektiert wurden.

  Im Beispiel würde beim Laden von Einzelobjekten aus der Tabelle RSECUSERAUTH jedes Auftreten der Variable $BNAME$ mit dem aktuellen Wert der Spalte USERNAME ersetzt werden, bevor die SQL-Selektion ausgeführt wird. Die Spalte USERNAME muss zuvor in einer Objektliste geladen worden sein.

  Tabellendefinitionen mit einem Mapping werden in erster Linie zum Laden von Einzelobjekten genutzt.
- Neben den selbst definierten Parametern können in Where-Klauseln auch vordefinierte Variablen genutzt werden. Weitere Informationen finden Sie unter Schemaerweiterungsdatei erstellen auf Seite 45.

Beispiel:

```
<Tables>
    <TABLE Definition = "HRP1001-Table" TableName="HRP1001"
    Key="OTJID,SUBTY,BEGDA,ENDDA" X500="CN,OU,OU,OU" SQL="MANDT = sy-mandt"
    Load="VARYF" Distinct="OTJID,SUBTY,VARYF" />
    <TABLE Definition = "HRP1000-Table" TableName="HRP1000"
    Key="OTJID,LANGU,BEGDA,ENDDA" X500="CN,OU,OU,OU" SQL="MANDT = sy-mandt" Load=""
    Distinct="OTJID" />
    <TABLE Definition = "RSECUSERAUTH-SingleUser" TableName="RSECUSERAUTH" Key="AUTH"
    X500="CN" SQL="UNAME = '$BNAME$'" Load="" >
        <Mapping>
            <Data ParameterName = "$BNAME$" PropertyName = "USERNAME" />
        </Mapping>
    </TABLE>
</Tables>
```

Funktionen definieren

Im Definitionsteil für Funktionen (`Functions`) werden die Schnittstellen zu den BAPI-Funktionen beschrieben, die zum Zugriff auf die Daten für die zu definierenden Schematypen benötigt werden.

Tabelle 19: Funktionsdefinition

Attribut	Beschreibung
Definition	Symbolischer Name zur Verwendung der Definition.
FunctionName	Funktionsname im SAP R/3-System.
OutStructure	Name einer SAP–Struktur, die als Rückgabewert geliefert wird. (Optional)
Key	Schlüsselbegriffe zur Bildung eines definierten Namens. Die Angabe von mehreren Werten als kommagetrennte Liste ist möglich.
X500	Kürzel für die Schlüsselbegriffe im Attribut `Key`. Die Angabe von mehreren Werten als kommagetrennte Liste ist möglich.

Im optionalen Mapping-Block wird definiert, wie die Werte an die Parameter des Funktionsaufrufs übergeben werden. Dazu muss vor dem Funktionsaufruf eine Objektliste erzeugt werden, aus deren Eigenschaften die Parameter für den Funktionsaufruf belegt werden können. Im Beispiel unten ist `BNAME` eine Eigenschaft, die über die Objektliste der Tabelle `USR02` ermittelt wird.

An die Parameter können vordefinierte Variablen übergeben werden. Weitere Informationen finden Sie unter Schemaerweiterungsdatei erstellen auf Seite 45. Außerdem ist es möglich, einem Funktionsparameter einen festen Wert zu übergeben. Dafür ist die folgende Notation vorgesehen.

```
<Data ParameterName = "<Name>" PropertyName = "VALUE=<fester Wert>" />
```

Beispiel:

```
<Tables>
     <TABLE Definition = "USR02-Table" TableName="USR02" Key="BNAME" X500="CN"
     SQL="MANDT = '$MANDT$'" Load="" />
</Tables>
<Functions>
     <Function Definition = "USER GET" FunctionName="BAPI_USER_GET_DETAIL"
     OutStructure = "" Key ="USERNAME" X500 ="CN">
          <Mapping>
               <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
          </Mapping>
```

```
    </Function>
</Functions>
```

Verwandte Themen

- Beispiel für eine Schemaerweiterungsdatei auf Seite 234

Schematypen definieren

Im Definitionsteil für Schematypen (`SAPExtendedSchematypes`) werden die Schematypen definiert, die im SAP Schema vorhanden sind und mit denen das Konnektorschema erweitert werden soll. Als Name wird der im Attribut `Name` vergebene Bezeichner verwendet. Dieser Bezeichner muss im erweiterten Konnektorschema eindeutig sein.

Tabelle 20: Schematypdefinition

Attribut	Beschreibung
Bem	Interne Beschreibung.
Name	Name des Schematyps im erweiterten Konnektorschema.
DisplayPattern	Definition eines Anzeigemusters für die Anzeige der Objekte im Synchronization Editor (beispielsweise im Zielsystembrowser oder bei der Definition der Schemaklassen). (Optional) Es können nur die Spalten verwendet werden, die in der Tabellendefinition geladen wurden (Attribute `Key` oder `Load`). WICHTIG: Jede Spalte, die beim Laden der Objektliste zusätzlich geladen werden muss, erzeugt zusätzliche Last im One Identity Manager. Bei großen Datenmengen kann die Synchronisation dadurch deutlich langsamer werden. Geben Sie hier nur Spalten an, die für die weitere Verarbeitung der Objekte zwingend benötigt werden.
AddRevisionTimeOffset	Gibt an, ob an den Revisionszähler die Uhrzeit **23:59:00** angefügt werden soll. (Optional) Sie können das Attribut nutzen, wenn der Revisionszähler nur ein Änderungsdatum und keine Uhrzeit enthält. Damit werden bei der Synchronisation auch solche Objekte berücksichtigt, die nach dem vorherigen Synchronisationslauf, aber noch am selben Tag geändert wurden.
RevisionProperty	Name einer Eigenschaft, welche den Revisionszähler enthält. (Optional)
ListObjectsDefinition	Funktions- oder Tabellendefinition zum Aufruf einer Objektliste.
ReadObjectDefinition	Funktions- oder Tabellendefinition zum Aufruf eines Einzelobjekts.

Attribut	Beschreibung
WriteObjectDefinition	Funktionsdefinition zum Schreiben des Objekts. (Optional)
DeleteObjectDefinition	Funktionsdefinition zum Löschen des Objekts. (Optional)
ParentType	Kontext, in dem der Schematyp gilt. (Optional) Standardmäßig sind die Schematypen mandantenbezogen (`ParentType="SAPMANDANT"`). Wenn der neue Schematyp in allen Mandanten eines SAP R/3-Systems gilt, geben Sie den `ParentType` mit dem Wert "SAPSYSTEM" an. Wenn das Attribut nicht definiert ist, ist der Schematyp mandantenbezogen.

Eine Schematypdefinition muss mindestens den Aufruf einer Objektliste (Attribut `ListObjectsDefinition`) enthalten. Dabei kann eine Tabellen- oder eine Funktionsdefinition angegeben werden. Um ein Einzelobjekt aufzurufen (Attribut `ReadObjectDefinition`), muss zuvor die Objektliste geladen worden sein. Listenaufruf und Einzelobjektaufruf können sich auf unterschiedliche Tabellen beziehen, jedoch müssen die Schlüsselspalten für die Identifikation der Einzelobjekte entweder gleichnamig sein oder per Mapping in der Tabellendefinition für den Einzelobjektaufruf bekannt gegeben worden sein. Im Beispiel unten werden zu einem Objekt aus der Tabelle `USR02` die Einzelobjekte aus der Tabelle `RSECUSERAUTH` ermittelt. Die Schlüsselspalten zur Identifikation der Objekte sind `USR02.BNAME` und `RSECUSERAUTH.UNAME`. Die Spalten haben unterschiedliche Namen und werden daher über den Parameter `$BNAME$` gemappt.

Es ist möglich, einen `Properties`–Block zu definieren, in welchem beliebig viele weitere Eigenschaften eines Objekts und die Art des Zugriffs auf diese Eigenschaften deklariert werden können. Eine einzelne Eigenschaft wird mittels `Property`-Tag definiert, welches die folgenden Attribute haben kann.

Tabelle 21: Eigenschaftsdefinition

Attribut	Beschreibung
Name	Name der Eigenschaft. Er muss innerhalb des Schematyps eindeutig sein.
Description	Beschreibung der Eigenschaft.
ListFunction	Funktion oder Tabelle zum Aufruf aller Werte.
AddFunction	Funktion zum Hinzufügen eines Wertes. (Optional)
DelFunction	Funktion zum Entfernen eines Wertes. (Optional)
ReplaceFunction	Ersetzen des gesamten Inhalts der Eigenschaft. (Optional)
IsMultivalued	Angabe, ob die Eigenschaft mehrwertig ist. (Optional) Wenn das Attribut nicht definiert ist, ist die Eigenschaft nicht mehrwertig.

Beispiel:

```
<Tables>
     <TABLE Definition = "USR04-Table" TableName="USR04" Key="BNAME,MANDT"
     X500="CN,OU" SQL="MANDT = sy-mandt" Load="" />
     <TABLE Definition = "USR02-Table" TableName="USR02" Key="BNAME" X500="CN"
     SQL="MANDT = sy-mandt" Load="MANDT,TRDAT" />
     <TABLE Definition = "RSECUSERAUTH-SingleUser" TableName="RSECUSERAUTH" Key="AUTH"
     X500="CN" SQL="UNAME = '$BNAME$'" Load="">
          <Mapping>
               <Data ParameterName = "$BNAME$" PropertyName = "BNAME" />
          </Mapping>
     </TABLE>
</Tables>
<Functions>
     <Function Definition = "USER GET" FunctionName="BAPI_USER_GET_DETAIL"
     OutStructure = "" Key ="USERNAME" X500 ="CN">
          <Mapping>
               <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
          </Mapping>
     </Function>
     <Function Definition = "USER SET" FunctionName="BAPI_USER_CHANGE" OutStructure
     ="" Key ="USERNAME" X500 ="CN">
          <Mapping>
               <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
          </Mapping>
     </Function>
     <Function Definition = "USER DEL" FunctionName="BAPI_USER_DELETE" OutStructure
     ="" Key ="USERNAME" X500 ="CN" >
          <Mapping>
               <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
          </Mapping>
     </Function>
     <Function Definition = "USER PROFILE SET" FunctionName="BAPI_USER_PROFILES_
     ASSIGN" OutStructure ="" Key ="USERNAME" X500 ="CN">
          <Mapping>
               <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
```

```
            <Data ParameterName = "BAPIPROF~BAPIPROF" PropertyName = "$Value$" />
        </Mapping>
    </Function>
    <Function Definition = "BWProfileDelFkt" FunctionName="/VIAENET/SAPHR_
    RSECUSERAUT_DEL" OutStructure ="" Key ="ZUSRNAME,ZHIER" X500 ="CN,OU">
        <Mapping>
            <Data ParameterName = "ZUSRNAME" PropertyName = "BNAME" />
            <Data ParameterName = "ZHIER" PropertyName = "$VALUE$" />
        </Mapping>
    </Function>
    <Function Definition = "BWProfileAddFkt" FunctionName="/VIAENET/SAPHR_
    RSECUSERAUT_ADD" OutStructure ="" Key ="ZUSRNAME,ZHIER" X500 ="CN,OU">
        <Mapping>
            <Data ParameterName = "ZUSRNAME" PropertyName = "BNAME" />
            <Data ParameterName = "ZHIER" PropertyName = "$VALUE$" />
        </Mapping>
    </Function>
</Functions>
<SAPExtendedSchematypes>
    <SAPExtendedSchematype Bem = "alle Benutzer" Name = "UserFunctionTable"
    DisplayPattern="%BNAME% (%MANDT%)" RevisionProperty="TRDAT" ListObjectsDefinition
    = "USR02-Table" ReadObjectDefinition ="USER GET" WriteObjectDefinition = "USER
    SET" DeleteObjectDefinition = "USER DEL">
        <Properties>
            <Property Name = "SAPBWP" Description="alle BW Profile des
            Benutzers" ListFunction="RSECUSERAUTH-SingleUser"
            AddFunction="BWProfileAddFkt" DelFunction="BWProfileDelFkt"
            ReplaceFunction="" IsMultivalued = "true" />
            <Property Name = "USERPROFILE" Description="alle Profile des
            Benutzers" ListFunction="USR04-Table" AddFunction="" DelFunction=""
            ReplaceFunction="USER PROFILE SET" IsMultivalued = "true" />
        </Properties>
    </SAPExtendedSchematype>
    <SAPExtendedSchematype Bem = "Asset, Anlagenwerte" Name = "Asset_ANLA"
    DisplayPattern="%ANLN1% %BUKRS%" AddRevisionTimeOffset="true"
    RevisionProperty="AEDAT" ListObjectsDefinition = "ANLA-Tabelle"
    ReadObjectDefinition = "ANLA-Tabelle" InsertObjectDefinition = ""
    WriteObjectDefinition = "" DeleteObjectDefinition = "" />
</SAPExtendedSchematypes>
```

Erläuterungen:

Die Liste von Objekten des Schematyps `UserFunctionTable` wird unter Nutzung der Tabelle `USR02` erstellt. Lesen, Schreiben und Löschen erfolgt mit den Funktionen des USER–BAPI, die jeweils als `Function` deklariert wurden.

Der Schematyp hat einen `Properties`-Block. Hier werden zwei weitere Eigenschaften definiert, die weder über die Tabellendefinition des Listenaufrufs noch über die Funktionsdefinition des Einzelobjektaufrufs zurückgegeben werden. Definiert wird eine mehrwertige Eigenschaft `SAPBWP`, deren Werte aus der Tabelle `RSECUSERAUTH` ermittelt werden. Die Einzelobjekte werden über die Spalten `USR02.BNAME` und `RSECUSERAUTH.UNAME` identifiziert. Zum Einfügen und Löschen von Werten werden BAPI-Aufrufe genutzt, die als Funktionen definiert wurden.

Die Eigenschaft `Userprofile` ist ein Beispiel für eine mehrwertige Eigenschaft, deren Werte beim Lesen aus einer Tabelle stammen (`USR04`) und die eine `Replace`–Funktion hat. Daher müssen immer alle Werte bei Änderungen angegeben werden, die in der Eigenschaft verbleiben sollen. Die Schreibfunktion ist die originale Funktion des USER-BAPI zum Setzen von Profilen am Benutzer (Funktionsdefinition für `BAPI_USER_PROFILES_ASSIGN`). Die Einzelobjekte werden über die Spalten `USR02.BNAME` und `USR04.BNAME` identifiziert. Da die Schlüsselspalten den gleichen Namen haben, wird an der Tabellendefinition kein Mapping benötigt.

Der Schematyp `Asset_ANLA` verwendet den Revisionszähler `AEDAT`, welcher nur ein Änderungsdatum enthält. An diesen Revisionszähler fügt der Konnektor die Uhrzeit **23:59:00** an (`AddRevisionTimeOffset="true"`).

Beschleunigung der Synchronisation durch Revisionsfilterung

Beim Start der Synchronisation werden alle zu synchronisierenden Objekte geladen. Ein Teil dieser Objekte wurde gegebenenfalls seit der letzten Synchronisation nicht geändert und muss daher bei der Synchronisation nicht verarbeitet werden. Indem nur solche Objekte geladen werden, die sich seit der letzten Synchronisation geändert haben, kann die Synchronisation beschleunigt werden. Zur Beschleunigung der Synchronisation nutzt der One Identity Manager die Revisionsfilterung.

SAP R/3 unterstützt die Revisionsfilterung. Als Revisionszähler wird das Datum der letzte Änderung der SAP Objekte genutzt. Jede Synchronisation speichert ihr letztes Ausführungsdatum als Revision in der One Identity Manager-Datenbank (Tabelle `DPRRevisionStore`, Spalte `Value`). Dieser Wert wird als Vergleichswert für die Revisionsfilterung bei der nächsten Synchronisation mit dem selben Workflow genutzt. Bei der Synchronisation mit diesem Workflow wird das Änderungsdatum der SAP Objekte mit der in der One Identity Manager-Datenbank gespeicherten Revision verglichen. Es werden nur noch die Objekte aus dem Zielsystem gelesen, die sich seit diesem Datum verändert haben.

HINWEIS: SAP Rollen erhalten als Änderungsinformation im Zielsystem das Datum der letzten Generierung der Rolle. Bei der Synchronisation mit Revisionsfilterung werden nur

die SAP Rollen in der Datenbank aktualisiert, die seit der letzten Synchronisation im Zielsystem erneut generiert wurden.

Die Revision wird zu Beginn einer Synchronisation ermittelt. Objekte, die durch die Synchronisation geändert werden, werden bei der nächsten Synchronisation nochmals geladen und überprüft. Die zweite Synchronisation nach der Initialsynchronisation ist daher noch nicht deutlich schneller.

Die Revisionsfilterung kann an den Workflows oder an den Startkonfigurationen zugelassen werden.

Um die Revisionsfilterung an einem Workflow zuzulassen

- Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
- Bearbeiten Sie die Eigenschaften des Workflows. Wählen Sie in der Auswahlliste **Revisionsfilterung** den Eintrag **Revisionsfilter nutzen**.

Um die Revisionsfilterung an einer Startkonfiguration zuzulassen

- Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
- Bearbeiten Sie die Eigenschaften der Startkonfiguration. Wählen Sie in der Auswahlliste **Revisionsfilterung** den Eintrag **Revisionsfilter nutzen**.

Detaillierte Informationen zum Thema

- One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation

Synchronisation von Sammelrollen

In der Tabelle `SAPUserInSAPRole` werden nur direkt zugewiesene Einzel- und Sammelrollen abgebildet. Die Zuordnungen von Einzelrollen an Sammelrollen sind in der Tabelle `SAPCollectionRPG` abgebildet. Über beide Tabellen zusammen kann ermittelt werden, welche Einzelrollen einem Benutzerkonto indirekt zugewiesen sind.

Für die Vererbung von Einzelrollen an Benutzerkonten gilt standardmäßig: Ist einem Benutzerkonto eine Einzelrolle zugewiesen und ist diese Einzelrolle Bestandteil einer Sammelrolle, die dem Benutzerkonto ebenfalls zugewiesen ist, dann wird die Einzelrolle nicht zusätzlich an das Benutzerkonto vererbt. Damit wird die Mitgliedschaft des Benutzerkontos in der Einzelrolle bei der Provisionierung von Gruppenmitgliedschaften in die SAP R/3-Umgebung entfernt. Bei der nächsten Synchronisation wird diese Mitgliedschaft in der One Identity Manager-Datenbank gelöscht oder als ausstehend markiert, je nach Konfiguration der Synchronisation.

Um zu verhindern, dass Mitgliedschaften in Einzelrollen entfernt werden, wenn die Einzelrollen Bestandteil von Sammelrollen sind

- Aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\SAPR3\KeepRedundantProfiles".

Einschränken der Synchronisationsobjekte über Benutzerrechte

Der One Identity Manager bietet die Möglichkeit die zu synchronisierenden Benutzerkonten und Gruppen über Benutzerrechte einzuschränken. Dabei werden nur die Benutzerkonten und Gruppen synchronisiert, auf die das Benutzerkonto, mit dem sich der SAP R/3 Konnektor am Zielsystem anmeldet, berechtigt ist. Alle übrigen Gruppen und Benutzerkonten werden aus der Userliste und Gruppenliste des Funktionsbausteins "/VIAENET/U" herausgefiltert. Soll nur ein kleiner Teil, der in der SAP R/3-Umgebung vorhandenen Benutzerkonten und Gruppen mit der One Identity Manager-Datenbank synchronisiert werden, kann die Synchronisation auf diese Weise beschleunigt werden.

Voraussetzungen

- Dem Benutzerkonto, mit dem sich der SAP R/3 Konnektor am Zielsystem anmeldet, sind in der SAP R/3-Umgebung im Berechtigungsobjekt S_USER_GRP, Merkmal CLASS genau die Gruppen zugewiesen, die synchronisiert werden sollen.
- Es gibt Benutzerkonten, denen eine dieser Gruppen in der SAP R/3-Umgebung als Benutzergruppe für die Berechtigungsprüfung (in den Logondaten) zugewiesen ist.

Bei der Synchronisation werden genau die Gruppen in die One Identity Manager-Datenbank eingelesen, auf die dem Benutzerkonto, mit dem sich der SAP R/3 Konnektor am Zielsystem anmeldet, im Berechtigungsobjekt S_USER_GRP Zugriff gewährt ist. Alle Benutzerkonten, denen eine dieser Gruppen als Benutzergruppe für die Berechtigungsprüfung zugewiesen ist, werden ebenfalls synchronisiert. Alle anderen Gruppen und Benutzerkonten werden bei der Synchronisation wie im Zielsystem nicht vorhandene Objekte behandelt.

Nachbehandlung ausstehender Objekte

Objekte, die im Zielsystem nicht vorhanden sind, können bei der Synchronisation in den One Identity Manager als ausstehend gekennzeichnet werden. Damit kann verhindert werden, dass Objekte aufgrund einer fehlerhaften Datensituation oder einer fehlerhaften Synchronisationskonfiguration gelöscht werden.

Ausstehende Objekte

- können im One Identity Manager nicht bearbeitet werden,
- werden bei jeder weiteren Synchronisation ignoriert,
- werden bei der Vererbungsberechnung ignoriert.

Das heißt, sämtliche Mitgliedschaften und Zuweisungen bleiben solange erhalten, bis die ausstehenden Objekte nachbearbeitet wurden.

Führen Sie dafür einen Zielsystemabgleich durch.

Um ausstehende Objekte nachzubearbeiten

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Zielsystemabgleich: SAP R/3**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp **SAP R/3** als Synchronisationstabellen zugewiesen sind.
2. Öffnen Sie auf dem Formular **Zielsystemabgleich**, in der Spalte **Tabelle/Objekt** den Knoten der Tabelle, für die sie ausstehende Objekte nachbearbeiten möchten.

   Es werden alle Objekte angezeigt, die als ausstehend markiert sind. Die Spalten **Letzter Protokolleintrag** und **Letzte ausgeführte Methode** zeigen den Zeitpunkt für den letzten Eintrag im Synchronisationsprotokoll und die dabei ausgeführte Verarbeitungsmethode. Der Eintrag **Kein Protokoll verfügbar** hat folgende Bedeutungen:

   - Das Synchronisationsprotokoll wurde bereits gelöscht.

     - ODER -
   - Im Zielsystem wurde eine Zuweisung aus einer Mitgliederliste gelöscht.

     Bei der Synchronisation wird das Basisobjekt der Zuordnung aktualisiert. Dafür erscheint ein Eintrag im Synchronisationsprotokoll. Der Eintrag in der Zuordnungstabelle wird als ausstehend markiert, es gibt jedoch keinen Eintrag im Synchronisationsprotokoll.
   - Im Zielsystem wurde ein Objekt gelöscht, das eine Mitgliederliste enthält.

     Bei der Synchronisation werden das Objekt und alle zugehörigen Einträge in Zuordnungstabellen als ausstehend markiert. Ein Eintrag im Synchronisationsprotokoll erscheint jedoch nur für das gelöschte Objekt.

   TIPP:

   Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

   a. Wählen Sie auf dem Formular für den Zielsystemabgleich das Objekt.

   b. Öffnen Sie das Kontextmenü und klicken Sie **Objekt anzeigen**.
3. Wählen Sie die Objekte, die Sie nachbearbeiten möchten. Mehrfachauswahl ist möglich.
4. Klicken Sie in der Formularsymbolleiste eins der folgenden Symbole, um die jeweilige Methode auszuführen.

Tabelle 22: Methoden zur Behandlung ausstehender Objekte

Symbol	Methode	Beschreibung
	Löschen	Das Objekt wird sofort in der One Identity Manager-Datenbank gelöscht. Eine Löschverzögerung wird nicht berücksichtigt. Die Markierung **Ausstehend** wird für das Objekt entfernt.

Symbol	Methode	Beschreibung
		Indirekte Mitgliedschaften können nicht gelöscht werden.
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung **Ausstehend** wird für das Objekt entfernt. Die Methode löst das Ereignis `HandleOutstanding` aus. Dadurch wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt. Voraussetzungen: • Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen. • Der Zielsystemkonnektor kann schreibend auf das Zielsystem zugreifen.
	Zurücksetzen	Die Markierung **Ausstehend** wird für das Objekt entfernt.

5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

HINWEIS: Standardmäßig werden die ausgewählten Objekte parallel verarbeitet. Damit wird die Ausführung der ausgewählten Methode beschleunigt. Wenn bei der Verarbeitung ein Fehler auftritt, wird die Aktion abgebrochen und alle Änderungen werden rückgängig gemacht.

Um den Fehler zu lokalisieren, muss die Massenverarbeitung der Objekte deaktiviert werden. Die Objekte werden damit nacheinander verarbeitet. Das fehlerhafte Objekt wird in der Fehlermeldung benannt. Alle Änderungen, die bis zum Auftreten des Fehlers vorgenommen wurden, werden gespeichert.

Um die Massenverarbeitung zu deaktivieren

- Deaktivieren Sie in der Formularsymbolleiste  .

Für die Synchronisation in kundenspezifische Tabellen müssen Sie den Zielsystemabgleich anpassen.

Um kundenspezifische Tabellen in den Zielsystemabgleich aufzunehmen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **SAP R/3**.
3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die kundenspezifischen Tabellen zu, für die Sie ausstehende Objekte behandeln möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die kundenspezifischen Tabellen, für die ausstehende Objekte in das

Zielsystem publiziert werden dürfen und aktivieren Sie die Option **Publizierbar**.

8. Speichern Sie die Änderungen.

HINWEIS: Damit ausstehende Objekte in der Nachbehandlung publiziert werden können, muss der Zielsystemkonnektor schreibend auf das Zielsystem zugreifen können. Das heißt, an der Zielsystemverbindung ist die Option **Verbindung darf nur gelesen werden** deaktiviert.

Provisionierung von Mitgliedschaften konfigurieren

Mitgliedschaften, beispielsweise von Benutzerkonten in Gruppen, werden in der One Identity Manager-Datenbank in Zuordnungstabellen gespeichert. Bei der Provisionierung von geänderten Mitgliedschaften werden möglicherweise Änderungen, die im Zielsystem vorgenommen wurden, überschrieben. Dieses Verhalten kann unter folgenden Bedingungen auftreten:

- Mitgliedschaften werden im Zielsystem in Form einer Liste als Eigenschaft eines Objekts gespeichert (Beispiel: Liste von Rollenzuordnungen in der Eigenschaft `AGR_NAME` am SAP R/3 `User`).
- Änderungen von Mitgliedschaften sind in beiden verbundenen Systemen zulässig.
- Ein Provisionierungsworkflow und Provisionierungsprozesse sind eingerichtet.

Wird eine Mitgliedschaft im One Identity Manager geändert, wird standardmäßig die komplette Mitgliederliste in das Zielsystem übertragen. Mitgliedschaften, die zuvor im Zielsystem hinzugefügt wurden, werden dabei entfernt; zuvor gelöschte Mitgliedschaften werden wieder eingefügt.

Um das zu verhindern, kann die Provisionierung so konfiguriert werden, dass nur die einzelne geänderte Mitgliedschaft in das Zielsystem provisioniert wird. Das entsprechende Verhalten wird für jede Zuordnungstabelle separat konfiguriert.

Um die Einzelprovisionierung von Mitgliedschaften zu ermöglichen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **SAP R/3**.
3. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
4. Wählen Sie die Zuordnungstabellen, für die Sie die Einzelprovisionierung ermöglichen möchten. Mehrfachauswahl ist möglich.
    - Die Option kann nur für Zuordnungstabellen aktiviert werden, deren Basistabelle eine Spalte `XDateSubItem` oder `CCC_XDateSubItem` hat.
    - Zuordnungstabellen, die im Mapping in einer virtuellen Schemaeigenschaft zusammengefasst sind, müssen identisch markiert werden.

5. Klicken Sie **Merge-Modus**.
6. Speichern Sie die Änderungen.

Für jede Zuordnungstabelle, die so gekennzeichnet ist, werden Änderungen, die im One Identity Manager vorgenommen werden, in einer separaten Tabelle gespeichert. Bei der Provisionierung der Änderungen wird die Mitgliederliste im Zielsystem mit den Einträgen in dieser Tabelle abgeglichen. Damit wird nicht die gesamte Mitgliederliste überschrieben, sondern nur die einzelne geänderte Mitgliedschaft provisioniert.

HINWEIS: Bei einer Synchronisation wird immer die komplette Mitgliederliste aktualisiert. Dabei werden Objekte mit Änderungen, deren Provisionierung noch nicht abgeschlossen ist, nicht verarbeitet. Diese Objekte werden im Synchronisationsprotokoll aufgezeichnet.

Die Einzelprovisionierung von Mitgliedschaften kann durch eine Bedingung eingeschränkt werden. Wenn für eine Tabelle der Merge-Modus deaktiviert wird, dann wird auch die Bedingung gelöscht. Tabellen, bei denen die Bedingung bearbeitet oder gelöscht wurde, sind durch folgendes Icon gekennzeichnet:  . Die originale Bedingung kann jederzeit wiederhergestellt werden.

Um die Standardbedingung wiederherzustellen

1. Wählen Sie die Zuordnungstabelle, für welche Sie die Bedingung wiederherstellen möchten.
2. Klicken Sie mit der rechten Maustaste auf die gewählte Zeile und wählen Sie im Kontextmenü **Originalwerte wiederherstellen**.
3. Speichern Sie die Änderungen.

Ausführliche Informationen zur Provisionierung von Mitgliedschaften finden Sie im One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation.

HINWEIS: Änderungen der Mitgliedschaften von Benutzerkonten in Einzelrollen werden **immer** einzeln provisioniert. Die Einzelprovisionierung kann daher für die Tabelle `SAPUserInSAPRole` nicht konfiguriert werden.

Beschleunigung der Provisionierung und Einzelobjektsynchronisation

Um Lastspitzen aufzufangen, kann die Verarbeitung der Prozesse zur Provisionierung und Einzelobjektsynchronisation auf mehrere Jobserver verteilt werden. Damit können die Provisionierung und Einzelobjektsynchronisation beschleunigt werden.

HINWEIS: Die Lastverteilung sollte nicht permanent für Provisionierungen oder Einzelobjektsynchronisationen eingesetzt werden. Durch die parallele Verarbeitung der Objekte kann es beispielsweise vorkommen, dass Abhängigkeiten nicht aufgelöst werden, da die referenzierten Objekte von einem anderen Jobserver noch nicht vollständig verarbeitet wurden.

Sobald die Lastverteilung nicht mehr benötigt wird, stellen Sie sicher, dass der Synchronisationsserver die Prozesse zur Provisionierung und Einzelobjektsynchronisation ausführt.

Um die Lastverteilung zu konfigurieren

1. Konfigurieren Sie die Server und geben Sie diese im One Identity Manager als Jobserver bekannt.
   - Weisen Sie diesen Jobservern die Serverfunktion **SAP R/3 Konnektor** zu.

   Alle Jobserver müssen auf den gleichen SAP Mandanten zugreifen können, wie der Synchronisationsserver für das jeweilige Basisobjekt.
2. Weisen Sie im Synchronization Editor an das Basisobjekt eine kundendefinierte Serverfunktion zu.

   Über diese Serverfunktion werden alle Jobserver identifiziert, welche für die Lastverteilung genutzt werden sollen.

   Wenn für das Basisobjekt noch keine kundendefinierte Serverfunktion vorhanden ist, erstellen Sie hier eine neue.

   Ausführliche Informationen zur Bearbeitung von Basisobjekten finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.
3. Weisen Sie diese Serverfunktion im Manager an alle Jobserver zu, welche die Prozesse zur Provisionierung und Einzelobjektsynchronisation für das Basisobjekt verarbeiten sollen.

   Wählen Sie nur die Jobserver, welche die gleiche Konfiguration wie der Synchronisationsserver des Basisobjekts haben.

Sobald alle Prozesse verarbeitet wurden, soll wieder der Synchronisationsserver die Provisionierung und Einzelobjektsynchronisation ausführen.

Um den Synchronisationsserver ohne Lastverteilung zu nutzen

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

Ausführliche Informationen zur Lastverteilung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Detaillierte Informationen zum Thema

- Bearbeiten eines Servers auf Seite 84

Unterstützung bei der Analyse von Synchronisationsproblemen

Für die Analyse von Problemen während der Synchronisation, beispielsweise unzureichender Performance, kann ein Bericht erzeugt werden. Der Bericht enthält Informationen wie beispielsweise:

- Ergebnisse der Konsistenzprüfung
- Einstellungen zur Revisionsfilterung
- Verwendeter Scope
- Analyse des Synchronisationspuffers
- Zugriffszeiten auf die Objekte in der One Identity Manager-Datenbank und im Zielsystem

Um den Synchronisationsanalysebericht zu erstellen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie das Menü **Hilfe | Synchronisationsanalysebericht erstellen** und beantworten Sie die Sicherheitsabfrage mit **Ja**.

   Die Generierung des Berichts nimmt einige Zeit in Anspruch. Er wird in einem separaten Fenster angezeigt.
3. Drucken Sie den Bericht oder Speichern Sie ihn in einem der verschiedenen Ausgabeformate.

Deaktivieren der Synchronisation

Regelmäßige Synchronisationen können nur gestartet werden, wenn das Synchronisationsprojekt und der Zeitplan aktiviert sind.

Um regelmäßige Synchronisationen zu verhindern

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Startkonfiguration und deaktivieren Sie den hinterlegten Zeitplan.

   Synchronisationen können nun nur noch manuell gestartet werden.

Ein aktiviertes Synchronisationsprojekt kann nur eingeschränkt bearbeitet werden. Sind Schemaänderungen notwendig, muss das Schema im Synchronisationsprojekt aktualisiert werden. Dabei wird das Synchronisationsprojekt deaktiviert und kann erneut bearbeitet werden.

Des Weiteren muss das Synchronisationsprojekt deaktiviert werden, wenn keinerlei Synchronisationen gestartet werden dürfen (auch nicht manuell).

Um das Synchronisationsprojekt zu deaktivieren

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie auf der Startseite die Ansicht **Allgemein**.
3. Klicken Sie **Projekt deaktivieren**.

Detaillierte Informationen zum Thema

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines SAP Mandanten auf Seite 23

3

Basisdaten für die Verwaltung einer SAP R/3-Umgebung

Für die Verwaltung einer SAP R/3-Umgebung im One Identity Manager sind folgende Basisdaten relevant.

- Konfigurationsparameter

  Über Konfigurationsparameter konfigurieren Sie die Grundeinstellungen zum Systemverhalten. Der One Identity Manager stellt für verschiedene Konfigurationsparameter Standardeinstellungen zur Verfügung. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.

  Die Konfigurationsparameter sind in den One Identity Manager Modulen definiert. Jedes One Identity Manager Modul kann zusätzliche Konfigurationsparameter installieren. Einen Überblick über alle Konfigurationsparameter finden Sie im Designer in der Kategorie **Basisdaten | Allgemein | Konfigurationsparameter**.

  Weitere Informationen finden Sie unter Konfigurationsparameter für die Verwaltung einer SAP R/3-Umgebung auf Seite 223.

- Kontendefinitionen

  Um im laufenden Betrieb Benutzerkonten automatisch an Personen zu vergeben, kennt der One Identity Manager Kontendefinitionen. Kontendefinitionen können für jedes Zielsystem erzeugt werden. Hat eine Person noch kein Benutzerkonto in einem Zielsystem, wird durch die Zuweisung der Kontendefinition an eine Person ein neues Benutzerkonto erzeugt.

  Weitere Informationen finden Sie unter Einrichten von Kontendefinitionen auf Seite 66.

- Kennwortrichtlinien

  Der One Identity Manager unterstützt Sie beim Erstellen von komplexen Kennwortrichtlinien beispielsweise für Systembenutzerkennwörter, das zentrale Kennwort von Personen sowie für Kennwörter für die einzelnen Zielsysteme. Kennwortrichtlinien werden sowohl bei der Eingabe eines Kennwortes durch den Anwender als auch bei der Generierung von Zufallskennwörtern angewendet.

In der Standardinstallation werden vordefinierte Kennwortrichtlinien mitgeliefert, die Sie nutzen können und bei Bedarf an Ihre Anforderungen anpassen können. Zusätzlich können Sie eigene Kennwortrichtlinien definieren.

Weitere Informationen finden Sie unter Kennwortrichtlinien für SAP Benutzerkonten auf Seite 105.

- Initiales Kennwort für neue Benutzerkonten

  Um das initiale Kennwort für Benutzerkonten zu vergeben, stehen Ihnen verschiedene Möglichkeiten zur Verfügung. Es kann das zentrale Kennwort der zugeordneten Person auf das Kennwort des Benutzerkontos abgebildet werden, es kann ein fest vorgegebenes Kennwort verwendet werden oder ein zufällig generiertes initiales Kennwort vergeben werden.

  Weitere Informationen finden Sie unter Initiales Kennwort für neue SAP Benutzerkonten auf Seite 116.

- E-Mail-Benachrichtigungen über die Anmeldeinformationen

  Bei Erstellung eines neuen Benutzerkontos werden die Anmeldeinformationen an definierte Empfänger versendet. Dabei werden zwei Benachrichtigungen versendet, die den Benutzernamen und das initiale Kennwort enthalten. Zur Erzeugung der Benachrichtigungen werden Mailvorlagen genutzt.

  Weitere Informationen finden Sie unter E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 118.

- Anmeldesprachen

  Den Benutzerkonten kann eine Standard-Anmeldesprache zugeordnet werden. Anmeldesprachen können durch die Synchronisation in die One Identity Manager-Datenbank eingelesen werden.

  Weitere Informationen finden Sie unter Anmeldesprachen auf Seite 103.

- Zielsystemtypen

  Zielsystemtypen werden für die Konfiguration des Zielsystemabgleichs benötigt. An den Zielsystemtypen werden die Tabellen gepflegt, die ausstehende Objekte enthalten können.

  Weitere Informationen finden Sie unter Nachbehandlung ausstehender Objekte auf Seite 56.

- Server

  Für die Verarbeitung der SAP R/3-spezifischen Prozesse im One Identity Manager muss der Synchronisationsserver mit seinen Serverfunktionen bekannt sein.

  Weitere Informationen finden Sie unter Bearbeiten eines Servers auf Seite 84.

- Zielsystemverantwortliche

  Im One Identity Manager ist eine Standardanwendungsrolle für die Zielsystemverantwortlichen vorhanden. Weisen Sie dieser Anwendungsrolle die Personen zu, die berechtigt sind, alle Mandanten im One Identity Manager zu bearbeiten.

Wenn Sie die Bearbeitungsrechte der Zielsystemverantwortlichen auf einzelne Mandanten einschränken wollen, definieren Sie weitere Anwendungsrollen. Die Anwendungsrollen müssen der Standardanwendungsrolle untergeordnet sein.

Weitere Informationen finden Sie unter Zielsystemverantwortliche auf Seite 90.

Einrichten von Kontendefinitionen

Um im laufenden Betrieb Benutzerkonten automatisch an Personen zu vergeben, kennt der One Identity Manager Kontendefinitionen. Kontendefinitionen können für jedes Zielsystem erzeugt werden. Hat eine Person noch kein Benutzerkonto in einem Zielsystem, wird durch die Zuweisung der Kontendefinition an eine Person ein neues Benutzerkonto erzeugt.

Aus den Personenstammdaten resultieren die Daten für das Benutzerkonto im jeweiligen Zielsystem. Die Personen müssen ein zentrales SAP Benutzerkonto besitzen. Über die primäre Zuordnung der Person zu einem Standort, einer Abteilung, einer Kostenstelle oder einer Geschäftsrolle und die Zuweisung der IT Betriebsdaten zu diesen Unternehmensstrukturen wird automatisch die Zuteilung der IT Betriebsdaten zum Benutzerkonto der Person geregelt. Die Verarbeitung erfolgt über Bildungsregeln. In der Standardinstallation sind vordefinierte Bildungsregeln zur Ermittlung der benötigten Daten für die Benutzerkonten enthalten. Bei Bedarf können Sie die Bildungsregeln kundenspezifisch anpassen.

Ausführliche Informationen zu Kontendefinitionen finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

- Erstellen einer Kontendefinition
- Erstellen der Automatisierungsgrade
- Erstellen einer Abbildungsvorschrift für IT Betriebsdaten
- Erfassen der IT Betriebsdaten
- Zuweisen der Kontendefinition an Personen
- Zuweisen der Kontendefinition an ein Zielsystem

Werden Benutzerkonten in der SAP R/3-Umgebung über die Zentrale Benutzerverwaltung (ZBV) administriert, dann können Kontendefinitionen genutzt werden, um den Benutzerkonten den Zugriff auf die Tochtersysteme und das Zentralsystem zu gewähren. Weitere Informationen finden Sie unter Zentrale Benutzerverwaltung im One Identity Manager auf Seite 133.

Erstellen einer Kontendefinition

Um eine Kontendefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

   Klicken Sie in der Ergebnisliste  .
3. Bearbeiten Sie die Stammdaten der Kontendefinition.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Stammdaten einer Kontendefinition auf Seite 67

Stammdaten einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 23: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet. Für eine Kontendefinition zum Erzeugen von Benutzerkonten wählen Sie **SAPUser**. Zum Gewähren des Zugriffs auf die Mandanten einer Zentralen Benutzerverwaltung (ZBV) wählen Sie **SAPUserMandant**.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte Kontendefinition	Vorausgesetzte Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch mitbestellt oder zugeordnet. Wenn die Kontendefinition den Zugriff auf Mandanten einer ZBV bereitstellen soll, ordnen Sie hier die Kontendefinition zu, mit der die Benutzerkonten im Zentralsystem erzeugt werden. Damit wird ein Benutzerkonto im Zentralsystem erzeugt, falls die Person noch kein Benutzerkonto hat.

Eigenschaft	Beschreibung
	Für eine Kontendefinition zum Erzeugen von Benutzerkonten lassen Sie die Angabe leer.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatisierungsgrad (initial)	Standardautomatisierungsgrad, der bei Neuanlage von Benutzerkonten standardmäßig verwendet werden soll. Wenn die Kontendefinition für das Tochtersystem einer ZBV gilt, ordnen Sie den Automatisierungsgrad **Unmanaged** zu.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Kontendefinition an Personen. Erfassen Sie einen Wert zwischen 0 und 1. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Leistungsposition	Leistungsposition, über welche die Kontendefinition im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.
IT Shop	Angabe, ob die Kontendefinition über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Personen und Rollen außerhalb des IT Shop zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von den Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig.
Automatische Zuweisung zu Personen	Angabe, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Beim Speichern wird die Kontendefinition an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine Person neu angelegt wird, erhält sie ebenfalls automatisch diese Kontendefinition. WICHTIG: Aktivieren Sie diese Option nur, wenn sichergestellt ist, dass alle aktuell in der Datenbank vorhandenen internen Personen sowie alle zukünftig neu hinzuzufügenden internen Personen ein Benutzerkonto in diesem Zielsystem erhalten sollen! Um die automatische Zuweisung der Kontendefinition an alle

Eigenschaft	Beschreibung
	Personen zu entfernen, deaktivieren Sie die Option. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.
Kontendefinition bei dauerhafter Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei zeitweiliger Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei verzögertem Löschen beibehalten	Angabe zur Zuweisung der Kontendefinition bei verzögertem Löschen von Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei Sicherheitsgefährdung beibehalten	Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Ressourcentyp	Ressourcentyp zur Gruppierung von Kontendefinitionen.
Freies Feld 01- Freies Feld 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Erstellen der Automatisierungsgrade

Für eine Kontendefinition legen Sie Automatisierungsgrade für die Behandlung der Benutzerkonten fest. Der Automatisierungsgrad eines Benutzerkontos entscheidet über den

Umfang der vererbten Eigenschaften der Person an das Benutzerkonto. So kann beispielsweise eine Person mehrere Benutzerkonten in einem Zielsystem besitzen:

- Standardbenutzerkonto, welches alle Eigenschaften über die Person erbt
- Administratives Benutzerkonto, das zwar mit der Person verbunden ist, aber keine Eigenschaften von der Person erben soll

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

- **Unmanaged**: Benutzerkonten mit dem Automatisierungsgrad **Unmanaged** erhalten eine Verbindung zur Person, erben jedoch keine weiteren Eigenschaften. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Person werden initial einige der Personeneigenschaften übernommen. Werden die Personeneigenschaften zu einem späteren Zeitpunkt geändert, dann werden diese Änderungen nicht an das Benutzerkonto weitergereicht.
- **Full managed**: Benutzerkonten mit dem Automatisierungsgrad **Full managed** erben definierte Eigenschaften der zugeordneten Person. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Person werden initial die Personeneigenschaften übernommen. Werden die Personeneigenschaften zu einem späteren Zeitpunkt geändert, dann werden diese Änderungen an das Benutzerkonto weitergereicht.

HINWEIS: Die Automatisierungsgrade **Full managed** und **Unmanaged** werden in Bildungsregeln ausgewertet. Die mitgelieferten Bildungsregeln können Sie im Designer unternehmensspezifisch anpassen.

Abhängig von Ihren Anforderungen können Sie weitere Automatisierungsgrade definieren. Die Bildungsregeln müssen Sie um die Vorgehensweise für die zusätzlichen Automatisierungsgrade erweitern.

Legen Sie für jeden Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll. Ausführliche Informationen zu Automatisierungsgraden finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

- Um die Berechtigungen zu entziehen, wenn eine Person deaktiviert, gelöscht oder als sicherheitsgefährdend eingestuft wird, können die Benutzerkonten der Person gesperrt werden. Wird die Person zu einem späteren Zeitpunkt wieder aktiviert, werden ihre Benutzerkonten ebenfalls wieder freigeschaltet.
- Zusätzlich kann die Vererbung der Gruppenmitgliedschaften definiert werden. Die Unterbrechung der Vererbung kann beispielsweise gewünscht sein, wenn die Benutzerkonten einer Person gesperrt sind und somit auch nicht in Gruppen Mitglied sein dürfen. Während dieser Zeit sollen keine Vererbungsvorgänge für diese Personen berechnet werden. Bestehende Gruppenmitgliedschaften werden dann gelöscht!

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Automatisierungsgrade zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Automatisierungsgrade zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Automatisierungsgrade.
5. Speichern Sie die Änderungen.

WICHTIG: Der Automatisierungsgrad **Unmanaged** wird beim Erstellen einer Kontendefinition automatisch zugewiesen und kann nicht entfernt werden.

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Automatisierungsgrades.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Stammdaten eines Automatisierungsgrades auf Seite 71

Stammdaten eines Automatisierungsgrades

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 24: Stammdaten eines Automatisierungsgrades

Eigenschaft	Beschreibung
Automatisierungsgrad	Bezeichnung des Automatisierungsgrades.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Betriebsdaten überschreibend	Angabe, ob Daten an Benutzerkonten, die sich aus den IT Betriebsdaten bilden, automatisch aktualisiert werden. Zulässige Werte sind: • **Niemals**: Die Daten werden nicht aktualisiert.

Eigenschaft	Beschreibung
	• **Immer**: Die Daten werden immer aktualisiert. • **Nur initial**: Die Daten werden nur initial ermittelt.
Gruppen bei zeitweiliger Deaktivierung beibehalten	Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei zeitweiliger Deaktivierung sperren	Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen gesperrt werden sollen.
Gruppen bei dauerhafter Deaktivierung beibehalten	Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei dauerhafter Deaktivierung sperren	Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen gesperrt werden sollen.
Gruppen bei verzögertem Löschen beibehalten	Angabe, ob die Benutzerkonten zum Löschen markierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei verzögertem Löschen sperren	Angabe, ob die Benutzerkonten zum Löschen markierter Personen gesperrt werden sollen.
Gruppen bei Sicherheitsgefährdung beibehalten	Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei Sicherheitsgefährdung sperren	Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen gesperrt werden sollen.
Gruppen bei deaktiviertem Benutzerkonto beibehalten	Angabe, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen.

Erstellen einer Abbildungsvorschrift für IT Betriebsdaten

Eine Kontendefinition legt fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über die primären Rollen einer Person ermittelt werden können.

Die folgenden IT Betriebsdaten werden in der Standardkonfiguration des One Identity Manager für das automatische Erzeugen und Ändern von Benutzerkonten für eine Person im Zielsystem verwendet.

- Gruppen erbbar
- Identität
- Privilegiertes Benutzerkonto

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **IT Betriebsdaten Abbildungsvorschrift bearbeiten** und erfassen Sie folgende Informationen.

Tabelle 25: Abbildungsvorschrift für IT Betriebsdaten

Eigenschaft	Beschreibung
Spalte	Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.
Quelle	Angabe, welche Rolle verwendet wird, um die Eigenschaften für das Benutzerkonto zu ermitteln. Zur Auswahl stehen: • Primäre Abteilung • Primärer Standort • Primäre Kostenstelle • Primäre Geschäftsrolle HINWEIS: Verwenden Sie die primäre Geschäftsrolle nur, wenn das Geschäftsrollenmodul vorhanden ist. • keine Angabe Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option **Immer Standardwert verwenden** setzen.
Standardwert	Standardwert der Eigenschaft für das Benutzerkonto einer Person, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann.
Immer Standardwert verwenden	Angabe, ob die Eigenschaft des Benutzerkontos immer mit dem Standardwert besetzt wird. Es erfolgt keine dynamische Ermittlung der IT Betriebsdaten aus einer Rolle.

Eigenschaft	Beschreibung
Benachrichtigung bei Verwendung des Standards	Angabe, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkontos mit Standardwerten** verwendet. Um die Mailvorlage zu ändern, passen Sie den Konfigurationsparameter **TargetSystem | SAPR3 | Accounts | MailTemplateDefaultValues** an.

4. Speichern Sie die Änderungen.

Erfassen der IT Betriebsdaten

Um für eine Person Benutzerkonten mit dem Automatisierungsgrad **Full managed** zu erzeugen, müssen die benötigten IT Betriebsdaten ermittelt werden. Welche IT Betriebsdaten für welches Zielsystem konkret verwendet werden sollen, wird an den Geschäftsrollen, Abteilungen, Kostenstellen oder Standorten definiert. Einer Person wird eine eine primäre Geschäftsrolle, eine primäre Abteilung, eine primäre Kostenstelle oder ein primärer Standort zugeordnet. Abhängig von dieser Zuordnung werden die gültigen IT Betriebsdaten ermittelt und für die Erstellung des Benutzerkontos verwendet. Können über die primären Rollen keine gültigen IT Betriebsdaten ermittelt werden, werden die Standardwerte verwendet.

Wenn in einem Zielsystem mehrere Kontendefinitionen für die Abbildung der Benutzerkonten verwendet werden, können Sie die IT Betriebsdaten auch direkt für eine konkrete Kontendefinition festlegen.

Beispiel

In der Regel erhält jede Person der Abteilung A ein Standardbenutzerkonto im Mandanten A. Zusätzlich erhalten einige Personen der Abteilung A administrative Benutzerkonten im Mandanten A.

Erstellen Sie eine Kontendefinition A für die Standardbenutzerkonten des Mandanten A und eine Kontendefinition B für die administrativen Benutzerkonten des Mandanten A. In der Abbildungsvorschrift der IT Betriebsdaten für die Kontendefinitionen A und B legen Sie die Eigenschaft "Abteilung" zur Ermittlung der gültigen IT Betriebsdaten fest.

Für die Abteilung A legen Sie die wirksamen IT Betriebsdaten für den Mandanten A fest. Diese IT Betriebsdaten werden für die Standardbenutzerkonten verwendet. Zusätzlich legen Sie für die Abteilung A die wirksamen IT Betriebsdaten für die Kontendefinition B fest. Diese IT Betriebsdaten werden für administrative Benutzerkonten verwendet.

Um IT Betriebsdaten festzulegen

1. Wählen Sie im Manager in der Kategorie **Organisationen** oder **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten**.
3. Klicken Sie **Hinzufügen** und erfassen Sie die folgenden Daten.

Tabelle 26: IT Betriebsdaten

Eigenschaft	Beschreibung
Wirksam für	Anwendungsbereich der IT Betriebsdaten. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden. Um den Anwendungsbereich festzulegen a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. b. Wählen Sie unter **Tabelle** die Tabelle, die das Zielsystem abbildet oder für eine Kontendefinition die Tabelle `TSBAccountDef`. c. Wählen Sie unter **Wirksam für** das konkrete Zielsystem oder die konkrete Kontendefinition. d. Klicken Sie **OK**.
Spalte	Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.
Wert	Konkreter Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.

4. Speichern Sie die Änderungen.

IT Betriebsdaten ändern

Sobald sich die IT Betriebsdaten ändern, müssen Sie diese Änderungen für bestehende Benutzerkonten übernehmen. Dafür führen Sie die Bildungsregeln an den betroffenen Spalten erneut aus. Bevor Sie die Bildungsregeln ausführen, prüfen Sie, welche Auswirkungen eine Änderung der IT Betriebsdaten auf bestehende Benutzerkonten hat. Für jede betroffene Spalte an jedem betroffenen Benutzerkonto können Sie entscheiden, ob die Änderung in die One Identity Manager-Datenbank übernommen werden soll.

Voraussetzungen

- Die IT Betriebsdaten einer Abteilung, einer Kostenstelle, einer Geschäftsrolle oder eines Standorts wurden geändert.

  - ODER -

- Die Standardwerte in der IT Betriebsdaten Abbildungsvorschrift für eine Kontendefinition wurden geändert.

HINWEIS: Ändert sich die Zuordnung einer Person zu einer primären Abteilung, Kostenstelle, Geschäftsrolle oder zu einem primären Standort, werden die Bildungsregeln automatisch ausgeführt.

Um die Bildungsregeln auszuführen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Bildungsregeln ausführen**.

   Es wird eine Liste aller Benutzerkonten angezeigt, die über die gewählte Kontendefinition entstanden sind und deren Eigenschaften durch die Änderung der IT Betriebsdaten geändert werden.

Alter Wert:	Aktueller Wert der Objekteigenschaft.
Neuer Wert:	Wert, den die Objekteigenschaft durch die Änderung an den IT Betriebsdaten annehmen würde.
Auswahl:	Angabe, ob die Änderung für das Benutzerkonto übernommen werden soll.

4. Markieren Sie in der Spalte **Auswahl** alle Objekteigenschaften, für die der neue Wert übernommen werden soll.
5. Klicken Sie **Übernehmen**.

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinition an Personen

Kontendefinitionen werden an die Personen des Unternehmens zugewiesen.

Das Standardverfahren für die Zuweisung von Kontendefinitionen an Personen ist die indirekte Zuweisung. Die Kontendefinitionen werden an die Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen zugewiesen. Die Personen werden gemäß ihrer Funktion im Unternehmen in diese Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen eingeordnet und erhalten so ihre Kontendefinitionen. Um auf Sonderanforderungen zu reagieren, können einzelne Kontendefinitionen direkt an Personen zugewiesen werden.

Kontendefinitionen können automatisch an alle Personen eines Unternehmens zugewiesen werden. Es ist möglich, die Kontendefinitionen als bestellbare Produkte dem IT Shop zuzuordnen. Der Abteilungsleiter kann dann für seine Mitarbeiter Benutzerkonten über das Web Portal bestellen. Zusätzlich ist es möglich, Kontendefinitionen in Systemrollen aufzunehmen. Diese Systemrollen können über hierarchische Rollen oder direkt an Personen zugewiesen werden oder als Produkte in den IT Shop aufgenommen werden.

In den Prozessen der One Identity Manager Standardinstallation wird zunächst überprüft, ob die Person bereits ein Benutzerkonto im Zielsystem der Kontendefinition besitzt. Ist kein Benutzerkonto vorhanden, so wird ein neues Benutzerkonto mit dem Standardautomatisierungsgrad der zugewiesenen Kontendefinition erzeugt.

HINWEIS: Ist bereits ein Benutzerkonto vorhanden und ist es deaktiviert, dann wird dieses Benutzerkonto entsperrt. Den Automatisierungsgrad des Benutzerkontos müssen Sie in diesem Fall nachträglich ändern.

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

- Für die Rollenklasse (Abteilung, Kostenstelle, Standort oder Geschäftsrolle) ist die Zuweisung von Personen und Kontendefinitionen erlaubt.

HINWEIS: Solange eine Kontendefinition für eine Person wirksam ist, behält die Person ihr daraus entstandenes Benutzerkonto. Wird die Zuweisung einer Kontendefinition entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht.

Ausführliche Informationen zur Vorbereitung der Rollenklassen für die Zuweisung finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Detaillierte Informationen zum Thema

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 77
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 78
- Kontendefinition an alle Personen zuweisen auf Seite 78
- Kontendefinition direkt an Personen zuweisen auf Seite 79
- Zuweisen der Kontendefinition an ein Zielsystem auf Seite 82

Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.

3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
    - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
    - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
    - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

    TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Organisationen entfernen.

    Um eine Zuweisung zu entfernen

    - Wählen Sie die Organisation und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Kontendefinition an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

    TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Geschäftsrollen entfernen.

    Um eine Zuweisung zu entfernen

    - Wählen Sie die Geschäftsrolle und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Kontendefinition an alle Personen zuweisen

Um eine Kontendefinition an alle Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung**

zu Personen.

WICHTIG: Aktivieren Sie diese Option nur, wenn sichergestellt ist, dass alle aktuell in der Datenbank vorhandenen internen Personen sowie alle zukünftig neu hinzuzufügenden internen Personen ein Benutzerkonto in diesem Zielsystem erhalten sollen!

5. Speichern Sie die Änderungen.

Die Kontendefinition wird an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine Person neu angelegt wird, erhält sie ebenfalls automatisch diese Kontendefinition. Die Zuweisung wird durch den DBQueue Prozessor berechnet.

HINWEIS: Um die automatische Zuweisung der Kontendefinition an alle Personen zu entfernen, deaktivieren Sie die Option **Automatische Zuweisung zu Personen**. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen bleiben jedoch erhalten.

Kontendefinition direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **An Personen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Personen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Person und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Kontendefinition an Systemrollen zuweisen

Installierte Module: Systemrollenmodul

HINWEIS: Kontendefinitionen, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können Sie nur an Systemrollen zuweisen, bei denen diese Option ebenfalls aktiviert ist.

Um Kontendefinitionen in eine Systemrolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemrollen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemrolle und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Kontendefinition in den IT Shop aufnehmen

Mit der Zuweisung einer Kontendefinition an ein IT Shop Regal kann sie von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Die Kontendefinition muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Kontendefinition muss eine Leistungsposition zugeordnet sein.

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Kontendefinition im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.
- Soll die Kontendefinition nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss sie zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen ist dann nicht mehr zulässig.

HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren Kontendefinitionen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Kontendefinition in den IT Shop aufzunehmen.

Um eine Kontendefinition in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   – ODER –

   Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontendefinition an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   – ODER –

   Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Kontendefinition aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   – ODER –

   Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionenn** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.

Ausführliche Informationen zur Bestellung von Unternehmensressourcen über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Verwandte Themen

- Stammdaten einer Kontendefinition auf Seite 67
- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 77
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 78
- Kontendefinition direkt an Personen zuweisen auf Seite 79
- Kontendefinition an Systemrollen zuweisen auf Seite 79

Zuweisen der Kontendefinition an ein Zielsystem

HINWEIS: Um die automatische Personenzuordnung für die Benutzerkonten einer Zentralen Benutzerverwaltung (ZBV) zu nutzen, weisen Sie dem Zentralsystem der ZBV eine Kontendefinition mit der Benutzerkontentabelle **SAPUser** zu.

Wenn Sie die automatische Zuordnung von Benutzerkonten und Personen einsetzen und dabei bereits verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen sollen, sind folgende Voraussetzungen zu gewährleisten:

- Die Kontendefinition ist dem Zielsystem zugewiesen.
- Die Kontendefinition besitzt einen Standardautomatisierungsgrad.

Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen Synchronisation der Fall.

Um die Kontendefinition an ein Zielsystem zuzuweisen

1. Wählen Sie im Manager in der Kategorie **SAP R/3 | Mandanten** den Mandanten.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie in der Auswahlliste **Kontendefinition (initial)** die Kontendefinition für die Benutzerkonten.
4. Speichern Sie die Änderungen.

Löschen einer Kontendefinition

Sie können Kontendefinitionen löschen, wenn diese keinem Zielsystem, keiner Person, keiner hierarchischen Rolle und keiner anderen Kontendefinition als Vorgänger zugeordnet sind.

Um eine Kontendefinition zu löschen

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Personen.
    a. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Deaktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.
    e. Speichern Sie die Änderungen.

2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Personen.
    a. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **An Personen zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Personen.
    e. Speichern Sie die Änderungen.
3. Entfernen Sie die Zuordnung der Kontendefinition zu Abteilungen, Kostenstellen und Standorten.
    a. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Organisationen zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Abteilungen, Kostenstellen und Standorte.
    e. Speichern Sie die Änderungen.
4. Entfernen Sie die Zuordnung der Kontendefinition zu Geschäftsrollen.
    a. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.

       Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
    d. Speichern Sie die Änderungen.
5. Wenn die Kontendefinition über den IT Shop bestellt wurde, muss sie abbestellt und aus allen IT Shop Regalen entfernt werden.

   Ausführliche Informationen zum Abbestellen einer Bestellung finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

   Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

    a. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

       – ODER –

       Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionenn** (bei rollenbasierter Anmeldung).
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
    d. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

e. Klicken Sie **OK**.

   Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.

6. Entfernen Sie die Zuordnung der Kontendefinition als vorausgesetzte Kontendefinition einer anderen Kontendefinition. Solange die Kontendefinition Voraussetzung einer anderen Kontendefinition ist, kann sie nicht gelöscht werden. Prüfen Sie alle Kontendefinitionen.
   a. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
   b. Wählen Sie in der Ergebnisliste die Kontendefinition.
   c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
   d. Entfernen Sie in der Auswahlliste **Vorausgesetzte Kontendefinition** die Kontendefinition.
   e. Speichern Sie die Änderungen.
7. Entfernen Sie die Zuordnung der Kontendefinition zum Zielsystem.
   a. Wählen Sie im Manager in der Kategorie **SAP R/3 | Mandanten** den Mandanten.
   b. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
   c. Entfernen Sie auf dem Tabreiter **Allgemein** die zugewiesenen Kontendefinitionen.
   d. Speichern Sie die Änderungen.
8. Löschen Sie die Kontendefinition.
   a. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
   b. Wählen Sie in der Ergebnisliste die Kontendefinition.
   c. Klicken Sie , um die Kontendefinition zu löschen.

Bearbeiten eines Servers

Für die Verarbeitung der SAP R/3-spezifischen Prozesse im One Identity Manager muss der Synchronisationsserver mit seinen Serverfunktionen bekannt sein. Um die Funktion eines Servers zu definieren, haben Sie mehrere Möglichkeiten:

- Erstellen Sie im Designer in der Kategorie **Basisdaten | Installationen | Jobserver** einen Eintrag für den Jobserver. Ausführliche Informationen dazu finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Wählen Sie im Manager in der Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Server** einen Eintrag für den Jobserver aus und bearbeiten Sie die Stammdaten des Jobservers.

Nutzen Sie dieses Verfahren, wenn der Jobserver bereits im One Identity Manager bekannt ist und Sie für den Jobserver spezielle Funktionen konfigurieren möchten.

HINWEIS: Damit ein Server seine Funktion im One Identity Manager Netzwerk ausführen kann, muss ein One Identity Manager Service installiert, konfiguriert und gestartet sein. Gehen Sie dazu wie im *One Identity Manager Installationshandbuch* beschrieben vor.

Um einen Jobserver und seine Funktionen zu bearbeiten

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Server**.
2. Wählen Sie in der Ergebnisliste den Jobserver-Eintrag.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für den Jobserver.
5. Wählen Sie die Aufgabe **Serverfunktionen zuweisen** und legen Sie die Serverfunktionen fest.
6. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Stammdaten eines Jobservers auf Seite 85
- Festlegen der Serverfunktionen auf Seite 88

Verwandte Themen

- Einrichten des Synchronisationsservers auf Seite 19

Stammdaten eines Jobservers

HINWEIS: Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten | Installationen | Jobserver** zur Verfügung.

HINWEIS: Abhängig von den installierten Modulen können weitere Eigenschaften verfügbar sein.

Tabelle 27: Eigenschaften eines Jobservers

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS Syntax. Beispiel: `<Name des Servers>.<Vollqualifizierter Domänenname>`

Eigenschaft	Bedeutung
Zielsystem	Zielsystem des Computerkontos.
Sprachkultur	Sprache des Servers.
Server ist Cluster	Angabe, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. HINWEIS: Die Eigenschaften **Server ist Cluster** und **Server gehört zu Cluster** schließen einander aus.
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.
IP-Adresse (IPv4)	Internet Protokoll Version 4 (IPv4)-Adresse des Servers.
Kopierverfahren (Quellserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Quelle einer Kopieraktion ist. Derzeit werden nur Kopierverfahren über die Programme `Robocopy` und `rsync` unterstützt. Wird kein Verfahren angegeben, ermittelt der One Identity Manager Service zur Laufzeit das Betriebssystem des Servers, auf dem die Kopieraktion ausgeführt wird. Die Replikation erfolgt dann zwischen Servern mit einem Windows Betriebssystem mit dem Programm `Robocopy` und zwischen Servern mit einem Linux Betriebssystem mit dem Programm `rsync`. Unterscheiden sich die Betriebssysteme des Quellservers und des Zielservers, so ist für eine erfolgreiche Replikation die Angabe der zulässigen Kopierverfahren zwingend erforderlich. Es wird das Kopierverfahren eingesetzt, das beide Server unterstützen.
Kopierverfahren (Zielserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Ziel einer Kopieraktion ist.
Codierung	Codierung des Zeichensatzes mit der Dateien auf dem Server geschrieben werden.
Übergeordneter Jobserver	Bezeichnung des übergeordneten Jobservers.
Ausführender Server	Bezeichnung des ausführenden Servers. Eingetragen wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden. Diese Angabe wird bei der automatischen Aktualisierung des One Identity Manager Service ausgewertet. Verarbeitet ein Server mehrere Queues, wird mit der Auslieferung von Prozessschritten solange gewartet, bis alle Queues, die auf demselben Server abgearbeitet werden, die automatische Aktualisierung abgeschlossen haben.
Queue	Bezeichnung der Queue, welche die Prozessschritte verarbeitet.

Eigenschaft	Bedeutung
	Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Serverbetriebssystem	Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte **Win32**, **Windows**, **Linux** und **Unix**. Ist die Angabe leer, wird **Win32** angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen.
One Identity Manager Service installiert	Angabe, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur `QBM_PJobQueueLoad` aktiviert, sobald die Queue das erste Mal angefragt wird. Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.
Stopp One Identity Manager Service	Angabe, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten. Den Dienst können Sie mit entsprechenden administrativen Rechten im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*.
Kein automatisches Softwareupdate	Angabe, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.
Softwareupdate läuft	Angabe, ob gerade eine Softwareaktualisierung ausgeführt wird.
Letzter Abrufzeitpunkt	Zeitpunkt der letzten Prozessabholung.
Letzte Timeout Prüfung	Zeitpunkt der letzten Prüfung für geladene Prozessschritte, deren Auslieferung den Wert im Konfigurationsparameter **Common |**

Eigenschaft	Bedeutung
	Jobservice | LoadedJobsTimeOut überschreitet.
Serverfunktion	Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

Verwandte Themen

- Festlegen der Serverfunktionen auf Seite 88

Festlegen der Serverfunktionen

HINWEIS: Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten | Installationen | Jobserver** zur Verfügung.

Die Serverfunktion definiert die Funktion eines Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

HINWEIS: Abhängig von den installierten Modulen können weitere Serverfunktionen verfügbar sein.

Tabelle 28: Zulässige Serverfunktionen

Serverfunktion	Anmerkungen
CSV Konnektor	Server, auf dem der CSV Konnektor für die Synchronisation installiert ist.
Domänen-Controller	Active Directory Domänen-Controller. Server, die nicht als Domänen-Controller gekennzeichnet sind, werden als Memberserver betrachtet.
Druckserver	Server, der als Druckserver arbeitet.
Generischer Server	Server für die generische Synchronisation mit einem kundendefinierten Zielsystem.
Homeserver	Server zur Anlage von Homeverzeichnissen für Benutzerkonten.
Aktualisierungsserver	Der Server führt die automatische Softwareaktualisierung aller anderen Server aus. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Der Server kann SQL Aufträge ausführen. Bei der initialen Schemainstallation wird der Server, auf dem die One Identity Manager-Datenbank installiert ist, mit dieser Serverfunktion gekennzeichnet.

Serverfunktion	Anmerkungen
SQL Ausführungsserver	Der Server kann SQL Aufträge ausführen. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Für eine Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.
CSV Skriptserver	Der Server kann CSV-Dateien per Prozesskomponente `ScriptComponent` verarbeiten.
Nativer Datenbankkonnektor	Der Server kann sich mit einer ADO.Net Datenbank verbinden.
One Identity Manager-Datenbankkonnektor	Server, auf dem der One Identity Manager Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem One Identity Manager aus.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
Primärer Domänen-Controller	Primärer Domänen-Controller.
Profilserver	Server für die Einrichtung von Profilverzeichnissen für Benutzerkonten.
SAM Synchronisationsserver	Server für die Synchronisation mit einem SMB-basierten Zielsystem aus.
SAP R/3 Konnektor	Server, auf dem der SAP R/3 Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem SAP R/3 aus.
SMTP Host	Server, auf dem durch den One Identity Manager Service E-Mail Benachrichtigungen verschickt werden. Voraussetzung zum Versenden von Mails durch den One Identity Manager Service ist ein konfigurierter SMTP Host.
Standard Berichtserver	Server, auf dem die Berichte generiert werden.
Windows PowerShell Konnektor	Der Server kann Windows PowerShell Version 3.0 oder neuer ausführen.

Verwandte Themen

- Stammdaten eines Jobservers auf Seite 85

Zielsystemverantwortliche

Im One Identity Manager ist eine Standardanwendungsrolle für die Zielsystemverantwortlichen vorhanden. Weisen Sie dieser Anwendungsrolle die Personen zu, die berechtigt sind, alle Mandanten im One Identity Manager zu bearbeiten.

Wenn Sie die Bearbeitungsrechte der Zielsystemverantwortlichen auf einzelne Mandanten einschränken wollen, definieren Sie weitere Anwendungsrollen. Die Anwendungsrollen müssen der Standardanwendungsrolle untergeordnet sein.

Ausführliche Informationen zum Einsatz und zur Bearbeitung von Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

1. Der One Identity Manager Administrator legt Personen als Zielsystemadministratoren fest.
2. Die Zielsystemadministratoren nehmen die Personen in die Standardanwendungsrolle für die Zielsystemverantwortlichen auf.

   Zielsystemverantwortliche der Standardanwendungsrolle sind berechtigt alle Mandanten im One Identity Manager zu bearbeiten.
3. Zielsystemverantwortliche können innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche berechtigen und bei Bedarf weitere untergeordnete Anwendungsrollen erstellen und einzelnen Mandanten zuweisen.

Tabelle 29: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | SAP R/3** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Systemberechtigungen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.

Benutzer	Aufgaben
	• Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Um initial Personen als Zielsystemadministrator festzulegen

1. Melden Sie sich als One Identity Manager Administrator (Anwendungsrolle **Basisrollen | Administratoren**) am Manager an.
2. Wählen Sie die Kategorie **One Identity Manager Administration | Zielsysteme | Administratoren**.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Person zu und speichern Sie die Änderung.

Um initial Personen in die Standardanwendungsrolle für Zielsystemverantwortliche aufzunehmen

1. Melden Sie sich als Zielsystemadministrator (Anwendungsrolle **Zielsysteme | Administratoren**) am Manager an.
2. Wählen Sie die Kategorie **One Identity Manager Administration | Zielsysteme | SAP R/3**.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Personen zu und speichern Sie die Änderungen.

Um als Zielsystemverantwortlicher weitere Personen als Zielsystemverantwortliche zu berechtigen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie in der Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Zielsystemverantwortliche** die Anwendungsrolle.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Personen zu und speichern Sie die Änderungen.

Um Zielsystemverantwortliche für einzelne Mandanten festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **SAP R/3 | Mandanten**.
3. Wählen Sie in der Ergebnisliste den Mandanten.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste

Zielsystemverantwortliche die Anwendungsrolle.

- ODER -

Klicken Sie neben der Auswahlliste **Zielsystemverantwortliche** auf , um eine neue Anwendungsrolle zu erstellen.

a. Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Zielsysteme | SAP R/3** zu.

b. Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.

6. Speichern Sie die Änderungen.
7. Weisen Sie der Anwendungsrolle die Personen zu, die berechtigt sind, den Mandanten im One Identity Manager zu bearbeiten.

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer SAP R/3-Umgebung auf Seite 12
- Allgemeine Stammdaten eines SAP Mandanten auf Seite 122

Basisdaten zur Benutzerverwaltung

Der One Identity Manager stellt folgende Basisdaten zur Benutzerverwaltung standardmäßig bereit:

- Benutzerkontentypen auf Seite 93
- Typen für externe Kennungen auf Seite 94

Weitere Basisdaten werden, sofern konfiguriert, während der Synchronisation aus der SAP R/3-Umgebung ausgelesen und können im One Identity Manager nicht bearbeitet werden. Diese dienen lediglich der Zuordnung zu einem SAP Benutzerkonto. Dazu gehören:

- SAP Parameter auf Seite 95
- Drucker auf Seite 102
- Kostenstellen auf Seite 102
- Startmenüs auf Seite 102
- Firmen auf Seite 103
- Anmeldesprachen auf Seite 103
- Lizenzen auf Seite 104
- Sonderversionen auf Seite 105

Bestimmte Eigenschaften von Benutzerkonten können über Konfigurationseinstellungen für alle Benutzerkonten einheitlich festgelegt werden. Dazu gehören:

- Initiales Kennwort für neue SAP Benutzerkonten auf Seite 116
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 118

Benutzerkontentypen

Die Benutzerkontentypen werden standardmäßig im One Identity Manager bereitgestellt. SAP R/3 kennt die nachfolgend aufgeführten Benutzerkontentypen.

Tabelle 30: Benutzerkontentypen

Benutzerkontentyp	Bedeutung
Dialog (A)	Dialognutzer in einem System.
System (B)	Dialogfreie Verarbeitung innerhalb eines Systems.
Kommunikation (C)	Dialogfreie Verarbeitung zwischen mehreren Systemen.
Service (S)	Allgemeines Benutzerkonto zum Beispiel für anonyme Systemzugänge. Benutzerkonten dieses Typs sollten stark eingeschränkte Berechtigungen besitzen.
Referenz (L)	Allgemeines Benutzerkonto für die zusätzliche Vergabe von Berechtigungen.

Im Konfigurationsparameter "TargetSystem\SAPR3\Accounts\Ustyp" ist der Standard-Benutzerkontentyp für neue Benutzerkonten festgelegt.

Um den Standard-Benutzerkontentyp zu ändern

- Bearbeiten Sie im Designer den Wert des Konfigurationsparameters "TargetSystem\SAPR3\Accounts\Ustyp".

Typen für externe Kennungen

In einer SAP R/3-Umgebung können externe Authentifizierungsmechanismen zu Anmeldung an einem System genutzt werden. Zur Ermittlung der Anmeldedaten, die bei den unterschiedlichen Authentifizierungsmechanismen externer Systeme an einem SAP System benötigt werden, liefert der One Identity Manager die folgenden Typen zur Kennzeichnung der Benutzerkonten mit.

Tabelle 31: Typen für externe Kennungen

Typ	Beschreibung
DN	Distinguished Name für X.509.
NT	Windows NTLM oder Kennwortverifizierung mit dem Windows-Domänen-Controller.
LD	LDAP-Bind <benutzerdefiniert> (Für andere externe Authentifizierungsmechanismen).
SA	SAML Token.

Um einen Standardtyp für externe Kennungen festzulegen

- Aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\SAPR3\Accounts\ExtID_Type" und legen Sie einen Wert fest.

SAP Parameter

Parameter können durch die Synchronisation in die One Identity Manager-Datenbank eingelesen und sowohl direkt als auch indirekt an Benutzerkonten zugewiesen werden. Bei der indirekten Zuweisung werden Personen und Parameter in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der Parameter, die einer Person zugewiesen ist. Wenn Sie eine Person in hierarchische Rollen aufnehmen und die Person ein Benutzerkonto besitzt, dann werden die Parameter an das Benutzerkonto zugewiesen.

Voraussetzung für die Zuweisung an die Benutzerkonten von Personen ist:

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und SAP Parametern erlaubt.
- Die Benutzerkonten und Parameter gehören zum selben SAP System.

Für jede hierarchische Rolle, an die ein Parameter zugewiesen ist, kann ein anderer Parameterwert festgelegt werden. Damit werden auch die Parameterwerte an die Benutzerkonten vererbt. Über die Zugehörigkeit zu hierarchischen Rollen kann so gesteuert werden, welche Parameterwerte die Parameter erhalten sollen, die den Benutzerkonten zugewiesen sind.

Detaillierte Informationen zum Thema

- Stammdaten für SAP Parameter anzeigen auf Seite 96
- Allgemeine Stammdaten für SAP Parameter auf Seite 96
- SAP Parameter an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 96
- SAP Parameter an Geschäftsrollen zuweisen auf Seite 98
- Parameterwerte für indirekte SAP Parameterzuweisungen bearbeiten auf Seite 99
- Vererbung von Parameterwerten an SAP Benutzerkonten auf Seite 100

Verwandte Themen

- SAP Parameter direkt zuweisen auf Seite 146

Stammdaten für SAP Parameter anzeigen

Um die Eigenschaften eines Parameters anzuzeigen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Parameter**.
2. Wählen Sie in der Ergebnisliste den Parameter.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Um einen Überblick über einen Parameter zu erhalten

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Parameter**.
2. Wählen Sie in der Ergebnisliste den Parameter.
3. Wählen Sie die Aufgabe **Überblick zum Parameter**.

Auf dem Überblicksformular eines Parameters können Sie mit einem Mausklick auf ein zugewiesenes Benutzerkonto das Stammdatenformular des Benutzerkontos öffnen. Hier können Sie den Parameterwert anpassen, mit dem diese Zuweisung modifiziert ist.

Detaillierte Informationen zum Thema

- SAP Parameter direkt zuweisen auf Seite 146

Allgemeine Stammdaten für SAP Parameter

Für Parameter werden folgende Eigenschaften abgebildet.

Tabelle 32: Eigenschaften eines Parameters

Eigenschaft	Beschreibung
System	System, zu dem der Parameter gehört.
Parameter	Bezeichnung des Parameters.
Text	Beschreibung des Parameters.

SAP Parameter an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie einen Parameter an Abteilungen, Kostenstellen oder Standorte zu, damit der Parameter über diese Organisationen an Benutzerkonten zugewiesen wird.

Um einen Parameter an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Parameter**.
2. Wählen Sie in der Ergebnisliste den Parameter.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Organisationen entfernen.

   Um eine Zuweisung zu entfernen
   - Wählen Sie die Organisation und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Um Parameter an eine Abteilung, eine Kostenstelle oder einen Standort zuzuweisen (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Organisationen | Abteilungen**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Organisationen | Kostenstellen**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **SAP Parameter zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Parameter zu. Um die angezeigten Parameter zu filtern, wählen Sie im Eingabefeld **SAP Systeme** ein System aus.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Parametern entfernen.

   Um eine Zuweisung zu entfernen
   - Wählen Sie den Parameter und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Parameter an Geschäftsrollen zuweisen auf Seite 98
- Parameterwerte für indirekte SAP Parameterzuweisungen bearbeiten auf Seite 99
- SAP Parameter direkt zuweisen auf Seite 146

- One Identity Manager Benutzer für die Verwaltung einer SAP R/3-Umgebung auf Seite 12

SAP Parameter an Geschäftsrollen zuweisen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.

Weisen Sie einen Parameter an Geschäftsrollen zu, damit der Parameter über diese Geschäftsrollen an Benutzerkonten zugewiesen wird.

Um einen Parameter an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Parameter**.
2. Wählen Sie in der Ergebnisliste den Parameter.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Geschäftsrollen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Um Parameter an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **SAP Parameter zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Parameter zu. Um die angezeigten Parameter zu filtern, wählen Sie im Eingabefeld **SAP Systeme** ein System aus.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Parametern entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Parameter und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Parameter an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 96
- Parameterwerte für indirekte SAP Parameterzuweisungen bearbeiten auf Seite 99
- SAP Parameter direkt zuweisen auf Seite 146
- One Identity Manager Benutzer für die Verwaltung einer SAP R/3-Umgebung auf Seite 12

Parameterwerte für indirekte SAP Parameterzuweisungen bearbeiten

Um für eine indirekte Parameterzuweisung einen Parameterwert zu erfassen, zu ändern oder zu löschen

1. Wählen Sie im Manager die Kategorie **Organisationen | Abteilungen**.
2. Wählen Sie in der Ergebnisliste die Abteilung, welcher der Parameter zugewiesen ist.
3. Wählen Sie die Aufgabe **Überblick über die Abteilung**.
4. Wählen Sie im Formularelement **SAP Parameter** den zugeordneten Parameter.

   Das Stammdatenformular der Parameterzuweisung wird geöffnet.
5. Erfassen, ändern oder löschen Sie den Parameterwert.
6. Speichern Sie die Änderungen.

- ODER -

1. Wählen Sie im Manager die Kategorie **Organisationen | Kostenstellen**.
2. Wählen Sie in der Ergebnisliste die Kostenstelle, welcher der Parameter zugewiesen ist.
3. Wählen Sie die Aufgabe **Überblick über die Kostenstelle**.
4. Wählen Sie im Formularelement **SAP Parameter** den zugeordneten Parameter.

   Das Stammdatenformular der Parameterzuweisung wird geöffnet.
5. Erfassen, ändern oder löschen Sie den Parameterwert.
6. Speichern Sie die Änderungen.

- ODER -

1. Wählen Sie im Manager die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste den Standort, welchem der Parameter zugewiesen ist.
3. Wählen Sie die Aufgabe **Überblick über den Standort**.

4. Wählen Sie im Formularelement **SAP Parameter** den zugeordneten Parameter.

   Das Stammdatenformular der Parameterzuweisung wird geöffnet.
5. Erfassen, ändern oder löschen Sie den Parameterwert.
6. Speichern Sie die Änderungen.

- ODER -

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle, welcher der Parameter zugewiesen ist.
3. Wählen Sie die Aufgabe **Überblick über die Geschäftsrolle**.
4. Wählen Sie im Formularelement **SAP Parameter** den zugeordneten Parameter.

   Das Stammdatenformular der Parameterzuweisung wird geöffnet.
5. Erfassen, ändern oder löschen Sie den Parameterwert.
6. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Parameter an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 96
- SAP Parameter an Geschäftsrollen zuweisen auf Seite 98
- SAP Parameter direkt zuweisen auf Seite 146
- Vererbung von Parameterwerten an SAP Benutzerkonten auf Seite 100

Vererbung von Parameterwerten an SAP Benutzerkonten

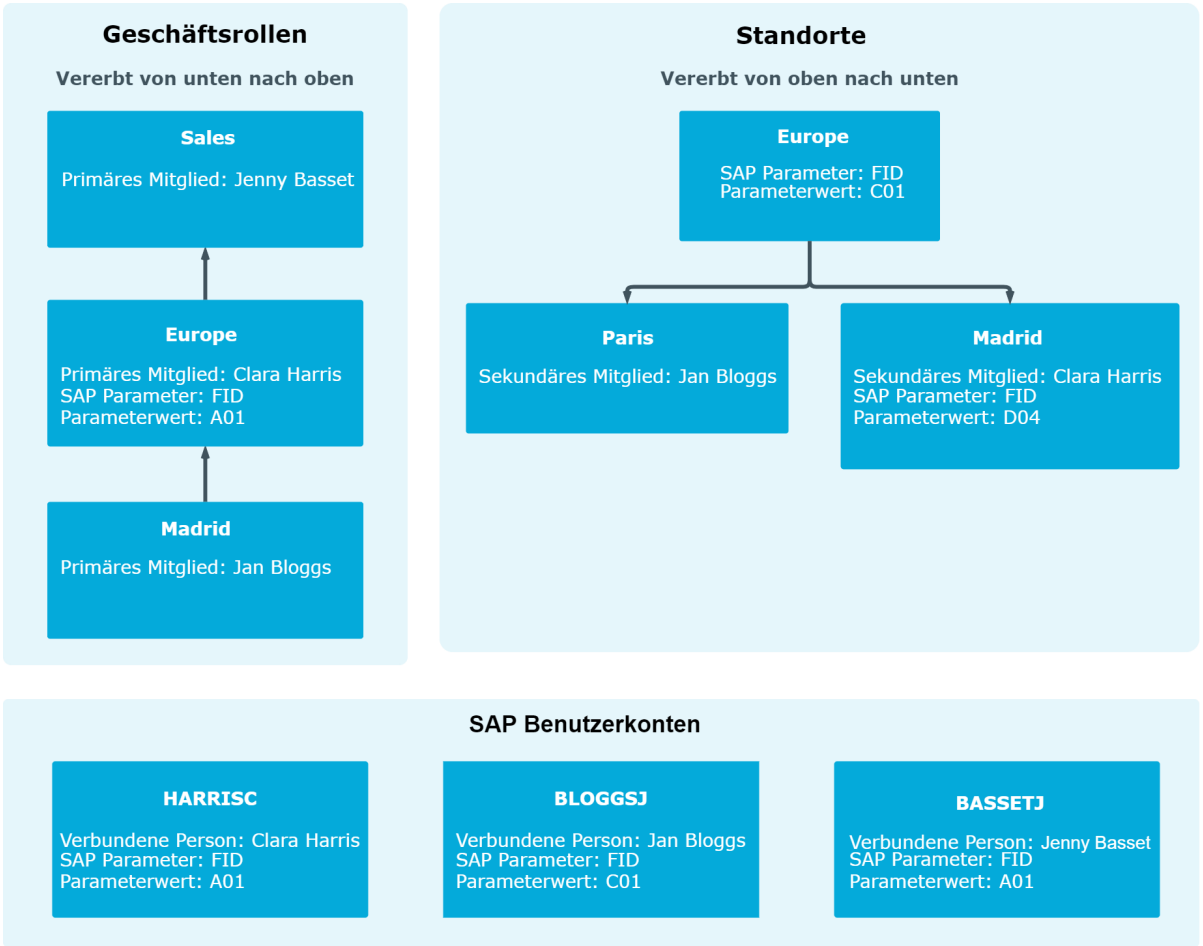
Bei der direkten Zuweisung von Parametern an Benutzerkonten kann ein Parameterwert erfasst werden. Ebenso kann bei der Zuweisung von Parametern an hierarchische Rollen ein Parameterwert festgelegt werden. Dieser Parameterwert wird mit dem Parameter an die Benutzerkonten vererbt. Wenn ein Parameter über verschiedene Wege an ein Benutzerkonto vererbt wird, dann wird der gültige Parameterwert folgendermaßen ermittelt:

1. Es werden die direkt zugewiesenen Parameter ermittelt.

   Direktzuweisungen entstehen durch:
   - Synchronisation der Benutzerkonten, inklusive ihrer Parameterzuweisungen
   - Direkte Zuweisung von Parametern im Manager

2. Es werden die indirekt zugewiesenen Parameter in folgender Reihenfolge ermittelt:
    a. primäre Abteilung
    b. primärer Standort
    c. primäre Kostenstelle
    d. primäre Geschäftsrolle
    e. sekundäre Abteilung
    f. sekundärer Standort
    g. sekundäre Kostenstelle
    h. sekundäre Geschäftsrolle
3. Wenn ein Parameter über verschiedene Rollen aus einer Rollenklasse vererbt wird, dann wird der gültige Parameterwert über den kürzesten Vererbungsweg in der Rollenhierarchie ermittelt. Dabei wird die an der Rollenklasse definierte Vererbungsrichtung berücksichtigt.

Abbildung 4: Beispiel für die Vererbung von SAP Parametern



Verwandte Themen

- Parameterwerte für indirekte SAP Parameterzuweisungen bearbeiten auf Seite 99
- SAP Parameter direkt zuweisen auf Seite 146

Drucker

Um einen Drucker anzuzeigen

1. Wählen Sie die Kategorie **SAP R/3 | Drucker**.
2. Wählen Sie in der Ergebnisliste den Drucker.

Auf dem Überblicksformular sind die Eigenschaften des Druckers, das zugeordnete SAP System und die zugeordneten Benutzerkonten abgebildet.

Kostenstellen

Um eine Kostenstelle anzuzeigen

1. Wählen Sie die Kategorie **SAP R/3 | Kostenstellen**.
2. Wählen Sie in der Ergebnisliste die Kostenstelle.

Auf dem Überblicksformular sind die Eigenschaften der Kostenstelle und der zugeordnete Mandant abgebildet.

Startmenüs

Um eine Startmenü anzuzeigen

1. Wählen Sie die Kategorie **SAP R/3 | Startmenüs**.
2. Wählen Sie in der Ergebnisliste das Startmenü.

Auf dem Überblicksformular sind die Eigenschaften des Startmenüs, der zugeordnete Mandant und die zugeordneten Benutzerkonten abgebildet.

Firmen

Um eine Firma anzuzeigen

1. Wählen Sie die Kategorie **SAP R/3 | Firmen**.
2. Wählen Sie in der Ergebnisliste die Firma.

Auf dem Überblicksformular sind die Eigenschaften der Firma, der zugeordnete Mandant und die zugeordneten Benutzerkonten abgebildet.

Anmeldesprachen

Um eine Anmeldesprache anzuzeigen

1. Wählen Sie die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Anmeldesprachen**.
2. Wählen Sie in der Ergebnisliste die Anmeldesprache.

Auf dem Überblicksformular sind die Eigenschaften der Anmeldesprache, das zugehörige SAP System und die zugeordneten Benutzerkonten abgebildet.

Sicherheitsrichtlinien

Sicherheitsrichtlinien können durch die Synchronisation in die One Identity Manager-Datenbank eingelesen und an Benutzerkonten zugewiesen werden.

Um Sicherheitsrichtlinien anzuzeigen

1. Wählen Sie die Kategorie **SAP R/3 | Sicherheitsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Sicherheitsrichtlinie. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Auf dem Überblicksformular sind die gültigen Sicherheitsrichtlinienattribute, der zugeordnete Mandant und die zugeordneten Benutzerkonten abgebildet.

Kommunikationsarten

Kommunikationsarten können durch die Synchronisation in die One Identity Manager-Datenbank eingelesen und an Benutzerkonten zugewiesen werden.

Um Kommunikationsarten anzuzeigen

1. Wählen Sie die Kategorie **SAP R/3 | Kommunikationsarten**.
2. Wählen Sie in der Ergebnisliste die Kommunikationsart.

Auf dem Überblicksformular sind die zugeordneten Benutzerkonten abgebildet.

Lizenzen

Lizenzen werden für die Systemvermessung der Benutzerkonten benötigt. Dafür kann für jede Lizenz eine Lizenzwertigkeit erfasst werden.

Um die Lizenzwertigkeit einer Lizenz zu erfassen

1. Wählen Sie die Kategorie **SAP R/3 | Lizenzen**.
2. Wählen Sie in der Ergebnisliste die Lizenz. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Erfassen Sie im Feld **Lizenzwertigkeit** einen Wert.
4. Speichern Sie die Änderungen.

Für eine Lizenz werden folgende Daten abgebildet:

Tabelle 33: Stammdaten einer Lizenz

Eigenschaft	Beschreibung
Lizenz	Eindeutige Kennung der Lizenz. Sie wird zur Ermittlung der Wertigkeit für die Systemvermessung genutzt, wenn keine Lizenzwertigkeit angegeben ist.
System	Zugehörigkeit zum SAP System.
Nutzertyp	Nutzertyp des SAP Systems, für den die Lizenz gültig ist.
Preisliste Kürzel	Nummer in der Preisliste.
Preisliste Text	Beschreibung in der Preisliste.
Lizenzwertigkeit	Wertigkeit der Lizenz als alphanumerische Zeichenkette. Erfassen Sie eine beliebige alphanumerische Zeichenkette. Bei der Ermittlung der Wertigkeit für die Systemvermessung wird nicht zwischen Groß- und Kleinschreibung unterschieden. Die Lizenzwertigkeit wird bei der Ermittlung der Wertigkeiten für die Systemvermessung ausgewertet. Ist keine Wertigkeit angegeben, wird die Kennung der Lizenz zur Ermittlung der Wertigkeit für die Systemvermessung genutzt.
Aktiviert	Angabe, ob die Lizenz aktiviert ist.

Eigenschaft	Beschreibung
Sonderversion	Angabe, ob für diese Lizenz Sonderversionen ausgewählt werden können.
Landeszuschlag	Angabe, ob für diese Lizenz Landeszuschläge ausgewählt werden können.

Detaillierte Informationen zum Thema

- Bereitstellen der Daten für die Systemvermessung auf Seite 210

Sonderversionen

Wenn in der SAP R/3-Umgebung Sonderversionen für Lizenzerweiterungen installiert sind, müssen die Benutzerkonten für die Systemvermessung entsprechend klassifiziert werden.

Auf dem Überblicksformular einer Sonderversion sehen Sie die Zuordnung zu den Benutzerkonten einer ZBV. Per Mausklick können Sie zu diesem Benutzerkonto navigieren und die Zuweisung der Sonderversion bearbeiten.

Um einen Überblick über eine Sonderversion zu erhalten

1. Wählen Sie die Kategorie **SAP R/3 | Sonderversionen**.
2. Wählen Sie in der Ergebnisliste die Sonderversion.

Kennwortrichtlinien für SAP Benutzerkonten

Der One Identity Manager unterstützt Sie beim Erstellen von komplexen Kennwortrichtlinien beispielsweise für Systembenutzerkennwörter, das zentrale Kennwort von Personen sowie für Kennwörter für die einzelnen Zielsysteme. Kennwortrichtlinien werden sowohl bei der Eingabe eines Kennwortes durch den Anwender als auch bei der Generierung von Zufallskennwörtern angewendet.

In der Standardinstallation werden vordefinierte Kennwortrichtlinien mitgeliefert, die Sie nutzen können und bei Bedarf an Ihre Anforderungen anpassen können. Zusätzlich können Sie eigene Kennwortrichtlinien definieren.

Detaillierte Informationen zum Thema

- Vordefinierte Kennwortrichtlinien auf Seite 106
- Anwenden einer Kennwortrichtlinie auf Seite 107

- Bearbeiten von Kennwortrichtlinien auf Seite 109
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 112
- Ausschlussliste für Kennwörter auf Seite 115
- Prüfen eines Kennwortes auf Seite 115
- Generieren eines Kennwortes testen auf Seite 116

Vordefinierte Kennwortrichtlinien

Die vordefinierte Kennwortrichtlinien können Sie bei Bedarf an Ihre Anforderungen anpassen.

Kennwortrichtlinie für die Anmeldung am One Identity Manager

Für die Anmeldung am One Identity Manager wird die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** angewendet. Diese Kennwortrichtlinie definiert die Einstellung für die Kennwörter von Systembenutzern (`DialogUser.Password` und `Person.DialogUserPassword`) sowie für den Zugangscode für die einmalige Anmeldung am Web Portal (`Person.Passcode`).

HINWEIS: Die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn keine andere Kennwortrichtlinie für Personen, Benutzerkonten oder Systembenutzer ermittelt werden kann.

Ausführliche Informationen zu Kennwortrichtlinien für Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Kennwortrichtlinie für die Bildung des zentralen Kennwortes von Personen

Bei entsprechender Konfiguration wird das zentrale Kennwort einer Person auf die Kennwörter der zielsystemspezifischen Benutzerkonten abgebildet. Die Kennwortrichtlinie **Kennwortrichtlinie für zentrales Kennwort von Personen** definiert die Einstellung für das zentrale Kennwort (`Person.CentralPassword`). Die Mitglieder der Anwendungsrolle **Identity Management | Personen | Administratoren** können diese Kennwortrichtlinie anpassen.

WICHTIG: Stellen Sie sicher, dass die Kennwortrichtlinie **Kennwortrichtlinie für zentrales Kennwort von Personen** nicht gegen die zielsystemspezifischen Anforderungen an Kennwörter verstößt.

Ausführliche Informationen zu Kennwortrichtlinien für Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Kennwortrichtlinien für Benutzerkonten

Es werden vordefinierte Kennwortrichtlinien bereitgestellt, die Sie auf die Kennwortspalten der Benutzerkonten anwenden können.

WICHTIG: Wenn Sie nicht mit zielsystemspezifischen Kennwortrichtlinien arbeiten, wirkt die Standardrichtlinie **One Identity Manager Kennwortrichtlinie**. Stellen Sie in diesem Fall sicher, dass die Standardrichtlinie nicht gegen die Anforderungen der Zielsysteme verstößt.

HINWEIS: Bei der Aktualisierung von One Identity Manager Version 7.x auf One Identity Manager Version 8.1.4 werden die Einstellung der Konfigurationsparameter zur Bildung von Kennwörtern auf die zielsystemspezifischen Kennwortrichtlinien umgesetzt.

Für SAP R/3 ist die Kennwortrichtlinie **SAP R/3 Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der SAP Benutzerkonten (`SAPUser.Password`) eines SAP Mandanten anwenden.

Wenn die Kennwortanforderungen der Mandanten unterschiedlich sind, wird empfohlen, je Mandant eine eigene Kennwortrichtlinie einzurichten.

Des Weiteren können Sie Kennwortrichtlinien abhängig von der Kontendefinition der Benutzerkonten oder abhängig vom Automatisierungsgrad der Benutzerkonten anwenden.

Anwenden einer Kennwortrichtlinie

Für SAP R/3 ist die Kennwortrichtlinie **SAP R/3 Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der SAP Benutzerkonten (`SAPUser.Password`) eines SAP Mandanten anwenden.

Wenn die Kennwortanforderungen der Mandanten unterschiedlich sind, wird empfohlen, je Mandant eine eigene Kennwortrichtlinie einzurichten.

Des Weiteren können Sie Kennwortrichtlinien abhängig von der Kontendefinition der Benutzerkonten oder abhängig vom Automatisierungsgrad der Benutzerkonten anwenden.

Die anzuwendende Kennwortrichtlinie für ein Benutzerkonto wird in folgender Reihenfolge ermittelt:

1. Kennwortrichtlinie der Kontendefinition des Benutzerkontos
2. Kennwortrichtlinie des Automatisierungsgrades des Benutzerkontos
3. Kennwortrichtlinie des Mandanten des Benutzerkontos
4. Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** (Standardrichtlinie)

WICHTIG: Wenn Sie nicht mit zielsystemspezifischen Kennwortrichtlinien arbeiten, wirkt die Standardrichtlinie **One Identity Manager Kennwortrichtlinie**. Stellen Sie in diesem Fall sicher, dass die Standardrichtlinie nicht gegen die Anforderungen der Zielsysteme verstößt.

Um eine Kennwortrichtlinie neu zuzuweisen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.

4. Klicken Sie im Bereich **Zuweisungen** die Schaltfläche **Hinzufügen** und erfassen Sie folgende Daten.

Tabelle 34: Zuweisen einer Kennwortrichtlinie

Eigenschaft	Beschreibung
Anwenden auf	Anwendungsbereich der Kennwortrichtlinie. ***Um den Anwendungsbereich festzulegen*** a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. b. Wählen Sie unter **Tabelle** eine der folgenden Referenzen: • Die Tabelle, die die Basisobjekte der Synchronisation enthält. • Um die Kennwortrichtlinie abhängig von der Kontendefinition anzuwenden, wählen Sie die Tabelle `TSBAccountDef`. • Um die Kennwortrichtlinie abhängig vom Automatisierungsgrad anzuwenden, wählen Sie die Tabelle `TSBBehavoir`. c. Wählen Sie unter **Anwenden auf** die Tabelle, die die Basisobjekte enthält. • Wenn Sie die Tabelle mit den Basisobjekten der Synchronisation gewählt haben, dann wählen Sie das konkrete Zielsystem. • Wenn Sie die Tabelle `TSBAccountDef` gewählt haben, dann wählen Sie die konkrete Kontendefinition. • Wenn Sie die Tabelle `TSBBehavior` gewählt haben, dann wählen Sie den konkreten Automatisierungsgrad. d. Klicken Sie **OK**.
Kennwortspalte	Bezeichnung der Kennwortspalte.
Kennwortrichtlinie	Bezeichnung der Kennwortrichtlinie, die angewendet werden soll.

5. Speichern Sie die Änderungen.

Um die Zuweisung einer Kennwortrichtlinie zu ändern

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.

4. Wählen Sie im Bereich **Zuweisungen** die Zuweisung, die Sie ändern möchten.
5. Wählen Sie in der Auswahlliste **Kennwortrichtlinie** die neu anzuwendende Kennwortrichtlinie.
6. Speichern Sie die Änderungen.

Bearbeiten von Kennwortrichtlinien

Um eine Kennwortrichtlinie zu bearbeiten

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie und wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Kennwortrichtlinie.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Kennwortrichtlinie auf Seite 109
- Richtlinieneinstellungen auf Seite 110
- Zeichenklassen für Kennwörter auf Seite 111
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 112

Allgemeine Stammdaten einer Kennwortrichtlinie

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 35: Stammdaten einer Kennwortrichtlinie

Eigenschaft	Bedeutung
Anzeigename	Bezeichnung der Kennwortrichtlinie. Übersetzen Sie den eingegebenen Text über die Schaltfläche .
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.Übersetzen Sie den eingegebenen Text über die Schaltfläche .
Fehlermeldung	Kundenspezifische Fehlermeldung, die ausgegeben wird, wenn die Richtlinie nicht erfüllt wird. Übersetzen Sie den eingegebenen Text über die Schaltfläche .

Eigenschaft	Bedeutung
Eigentümer (Anwendungsrolle)	Anwendungsrolle, deren Mitglieder die Kennwortrichtlinie konfigurieren können.
Standardrichtlinie	Kennzeichnung als Standardrichtlinie für Kennwörter. HINWEIS: Die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn keine andere Kennwortrichtlinie für Personen, Benutzerkonten oder Systembenutzer ermittelt werden kann.

Richtlinieneinstellungen

Auf dem Tabreiter **Kennwort** definieren Sie folgende Einstellungen für eine Kennwortrichtlinie.

Tabelle 36: Richtlinieneinstellungen

Eigenschaft	Bedeutung
Initiales Kennwort	Initiales Kennwort für neu erzeugte Benutzerkonten. Wird beim Erstellen eines Benutzerkontos kein Kennwort angegeben oder kein Zufallskennwort generiert, dann wird das initiale Kennwort benutzt.
Kennwortbestätigung	Kennwortwiederholung.
Min. Länge	Minimale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben muss.
Max. Länge	Maximale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben kann. Der maximal zulässige Wert ist **256**.
Max. Fehlanmeldungen	Anzahl der maximalen Fehlanmeldungen. Legen Sie die Anzahl der ungültigen Kennworteingaben fest. Wird nur berücksichtigt, bei Anmeldung am One Identity Manager. Die Angabe wird nur berücksichtigt, wenn die Anmeldung am One Identity Manager mit einem Systembenutzer- oder Personen-basierten Authentifizierungsmodul erfolgt. Hat ein Benutzer die Anzahl der maximalen Fehlanmeldungen erreicht, kann sich die Person oder der Systembenutzer nicht mehr am One Identity Manager anmelden. Kennwörter gesperrter Personen und Systembenutzer können im Kennwortrücksetzungsportal zurückgesetzt werden. Ausführliche Informationen finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

Eigenschaft	Bedeutung
Max. Tage gültig	Maximales Alter des Kennwortes. Geben Sie die Zeitspanne an, in der ein Kennwort verwendet werden kann, bevor ein neues Kennwort erwartet wird.
Kennwortchronik	Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert **5** eingegeben, werden die letzten fünf Kennwörter des Benutzers gespeichert.
Min. Kennwortstärke	Angabe, wie sicher ein Kennwort sein muss. Je höher die Kennwortstärke, desto sicherer ist das Kennwort. Mit dem Wert **0** wird die Kennwortstärke nicht geprüft. Die Werte **1**, **2**, **3** und **4** geben die erforderliche Komplexität des Kennwortes an. Dabei stellt der Wert **1** die geringsten Anforderungen an die Komplexität eines Kennwortes. Der Wert **4** fordert die höchste Komplexität.
Namensbestandteile unzulässig	Angabe, ob Namensbestandteile im Kennwort zulässig oder unzulässig sind. Ist die Option aktiviert, sind Namensbestandteile in Kennwörtern nicht zulässig. Es werden die Werte der Spalten berücksichtigt, für welche die Option **Enthält Namensbestandteile für die Kennwortprüfung** aktiviert ist. Die Option passen Sie im Designer an der Spaltendefinition an. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Zeichenklassen für Kennwörter

Auf dem Tabreiter **Zeichenklassen** legen Sie fest, welche Zeichen für ein Kennwort zulässig sind.

Tabelle 37: Zeichenklassen für Kennwörter

Eigenschaft	Bedeutung
Min. Anzahl Buchstaben	Angabe, wie viele alphabetische Zeichen ein Kennwort mindestens enthalten muss.
Min. Anzahl Kleinbuchstaben	Angabe, wie viele Kleinbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Großbuchstaben	Angabe, wie viele Großbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Ziffern	Angabe, wie viele Ziffern ein Kennwort mindestens enthalten muss.
Min. Anzahl Sonderzeichen	Angabe, wie viele Sonderzeichen ein Kennwort mindestens enthalten muss.

Eigenschaft	Bedeutung
Zulässige Sonderzeichen	Liste zulässiger Sonderzeichen.
Max. identische Zeichen insgesamt	Maximale Anzahl identischer Zeichen, die insgesamt im Kennwort vorkommen dürfen.
Max. identische Zeichen aufeinanderfolgend	Maximale Anzahl identischer Zeichen, die nacheinander wiederholt werden können.
Unzulässige Sonderzeichen	Liste unzulässiger Sonderzeichen.
Keine Kleinbuchstaben erzeugen	Angabe, ob ein generiertes Kennwort Kleinbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keinen Großbuchstaben erzeugen	Angabe, ob ein generiertes Kennwort Großbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keine Ziffern erzeugen	Angabe, ob ein generiertes Kennwort Ziffern enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keine Sonderzeichen erzeugen	Angabe, ob ein generiertes Kennwort Sonderzeichen enthalten darf. Ist die Option aktiviert, sind nur Buchstaben, Zahlen und Leerzeichen in Kennwörtern erlaubt. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.

Kundenspezifische Skripte für Kennwortanforderungen

Kundenspezifische Skripte zum Prüfen und Generieren von Kennwörtern können Sie einsetzen, wenn die Anforderungen an Kennwörter mit den vorhandenen Einstellmöglichkeiten nicht abgebildet werden können. Skripte werden zusätzlich zu den anderen Einstellungen angewendet.

Detaillierte Informationen zum Thema

- Skript zum Prüfen eines Kennwortes auf Seite 113
- Skript zum Generieren eines Kennwortes auf Seite 114

Skript zum Prüfen eines Kennwortes

Ein Prüfskript können Sie einsetzen, wenn zusätzliche Richtlinien beim Prüfen eines Kennwortes angewendet werden sollen, die nicht mit den vorhandenen Einstellmöglichkeiten abgebildet werden können.

Syntax für Prüfskripte

```
Public Sub CCC_CustomPwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
```

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Kennwort, das zu prüfen ist

TIPP: Um das Basisobjekt zu verwenden, nutzen Sie die Eigenschaft `Entity` der `PasswordPolicy`-Klasse.

Beispiel für ein Skript zum Prüfen eines Kennwortes

Ein Kennwort in darf nicht mit **?** oder **!** beginnen. Das Kennwort darf nicht mit drei identischen Zeichen beginnen. Das Skript prüft ein gegebenes Kennwort auf Zulässigkeit.

```
Public Sub CCC_PwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            Throw New Exception(#LD("Password can't start with '?' or '!'")#)
        End If
    End If
    If pwd.Length>2
        If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
            Throw New Exception(#LD("Invalid character sequence in password")#)
        End If
    End If
End Sub
```

Um ein kundenspezifisches Skript zum Prüfen eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kennwortrichtlinien.**

b. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.

c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

d. Tragen Sie auf dem Tabreiter **Skripte** im Eingabefeld **Prüfskript** den Namen des Skriptes ein, das zum Prüfen eines Kennwortes verwendet wird.

e. Speichern Sie die Änderungen.

Verwandte Themen

- Skript zum Generieren eines Kennwortes auf Seite 114

Skript zum Generieren eines Kennwortes

Ein Generierungsskript können Sie einsetzen, wenn zusätzliche Richtlinien beim Generieren eines Zufallskennwortes angewendet werden sollen, die nicht mit den vorhandenen Einstellmöglichkeiten abgebildet werden können.

Syntax für Generierungsskripte

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)
```

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Generiertes Kennwort

TIPP: Um das Basisobjekt zu verwenden, nutzen Sie die Eigenschaft `Entity` der `PasswordPolicy`-Klasse.

Beispiel für ein Skript zum Generieren eines Kennwortes

Das Skript ersetzt in Zufallskennwörtern die unzulässigen Zeichen **?** und **!** zu Beginn eines Kennwortes mit **_**.

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    ' replace invalid characters at first position
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            spwd.SetAt(0, CChar("_"))
        End If
    End If
End Sub
```

Um ein kundenspezifisches Skript zum Generieren eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
    b. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Tragen Sie auf dem Tabreiter **Skripte** im Eingabefeld **Generierungsskript** den Namen des Skriptes ein, das zum Generieren eines Kennwortes verwendet wird.
    e. Speichern Sie die Änderungen.

Verwandte Themen

- Skript zum Prüfen eines Kennwortes auf Seite 113

Ausschlussliste für Kennwörter

Um bestimmte Begriffe im Kennwort zu verbieten, nehmen Sie den Begriff in die Ausschlussliste auf.

HINWEIS: Die Ausschlussliste ist global für alle Kennwortrichtlinien gültig.

Um einen Begriff in die Ausschlussliste aufzunehmen

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | Kennwort Ausschlussliste**.
2. Erstellen Sie einen neuen Eintrag über den Menüeintrag **Objekt | Neu** und erfassen Sie den auszuschließenden Begriff.
3. Speichern Sie die Änderungen.

Prüfen eines Kennwortes

Beim Prüfen eines Kennwortes werden alle definierten Einstellungen der Kennwortrichtlinie, kundenspezifische Skripte sowie die Ausschlussliste für Kennwörter berücksichtigt.

Um zu prüfen, ob ein Kennwort der Kennwortrichtlinie entspricht

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Test**.
5. Wählen Sie in der Auswahlliste **Basisobjekt für den Test** die Tabelle und das Objekt für die Prüfung.
6. Geben Sie im Eingabefeld **Kennwort überprüfen** das Kennwort ein.

   Neben dem Eingabefeld wird angezeigt, ob das Kennwort gültig ist.

Generieren eines Kennwortes testen

Beim Generieren eines Kennwortes werden alle definierten Einstellungen der Kennwortrichtlinie, kundenspezifische Skripte sowie die Ausschlussliste für Kennwörter berücksichtigt.

Um ein Kennwort zu generieren, das der Kennwortrichtlinie entspricht

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Test**.
5. Klicken Sie auf die Schaltfläche **Generieren**.

   Das generierte Kennwort wird angezeigt.

Initiales Kennwort für neue SAP Benutzerkonten

Tabelle 38: Konfigurationsparameter für die Bildung eines initialen Kennwortes für Benutzerkonten

Konfigurationsparameter	Bedeutung
QER\Person\UseCentralPassword	Der Konfigurationsparameter legt fest, ob das zentrale Kennwort einer Person in den Benutzerkonten

Konfigurationsparameter	Bedeutung
	verwendet werden soll. Das zentrale Kennwort der Person wird automatisch auf die Benutzerkonten der Person in allen erlaubten Zielsystemen abgebildet. Ausgenommen sind privilegierte Benutzerkonten; diese werden nicht aktualisiert.
QER\Person\UseCentralPassword\PermanentStore	Der Konfigurationsparameter steuert die Aufbewahrungszeit der zentralen Kennworte. Ist der Konfigurationsparameter aktiviert, wird das zentrale Kennwort in der One Identity Manager-Datenbank gespeichert und wird für neue Benutzerkonten genutzt. Ist der Konfigurationsparameter deaktiviert, wird das zentrale Kennwort nach dem Publizieren an die bestehenden Benutzerkonten aus der One Identity Manager-Datenbank gelöscht werden. Das zentrale Kennwort steht für weitere Benutzerkonten nicht zur Verfügung.
TargetSystem\SAPR3\Accounts\ InitialRandomPassword	Der Konfigurationsparameter legt fest, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in der zugewiesenen Kennwortrichtlinie definiert sind.

Um das initiale Kennwort für neue SAP Benutzerkonten zu vergeben, stehen Ihnen verschiedene Möglichkeiten zur Verfügung.

- Erstellen Sie Benutzerkonten manuell und tragen Sie in den Stammdaten der Benutzerkonten ein Kennwort ein.
- Vergeben Sie beim Erstellen von Benutzerkonten ein zufällig generiertes initiales Kennwort.
  - Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | SAPR3 | Accounts | InitialRandomPassword**.
  - Verwenden Sie zielsystemspezifische Kennwortrichtlinien und definieren Sie in den Kennwortrichtlinien die Zeichenklassen, die das Kennwort enthalten muss.

- Legen Sie fest, an welche Person das initiale Kennwort per E-Mail versendet wird.

- Verwenden Sie das zentrale Kennwort der Person. Das zentrale Kennwort der zugeordneten Person wird auf das Kennwort des Benutzerkontos abgebildet. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- Kennwortrichtlinien für SAP Benutzerkonten auf Seite 105
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 118

E-Mail-Benachrichtigungen über Anmeldeinformationen

Tabelle 39: Konfigurationsparameter für Benachrichtigungen über Aktionen im Zielsystem

Konfigurationsparameter	Bedeutung
TargetSystem\SAPR3\Accounts\ InitialRandomPassword\SendTo	Der Konfigurationsparameter enthält die Person, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Geschäftsrolle, Verantwortlicher der Person oder `XUserInserted`). Ist kein Empfänger ermittelbar, dann wird an die im Konfigurationsparameter "TargetSystem\SAPR3\DefaultAddress" hinterlegte Adresse versandt.
TargetSystem\SAPR3\Accounts\ InitialRandomPassword\SendTo\ MailTemplateAccountName	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den Anmeldeinformationen zum Benutzerkonto zu versorgen. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto** verwendet.
TargetSystem\SAPR3\Accounts\ InitialRandomPassword\SendTo\ MailTemplatePassword	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den Informationen zum initialen Kennwort zu versorgen. Es wird die Mailvorlage **Person - Initiales Kennwort für neues Benutzerkonto** verwendet.
TargetSystem\SAPR3\DefaultAddress	Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem.

Die Anmeldeinformationen für neue Benutzerkonten können per E-Mail an eine festgelegte Person gesendet werden. Dabei werden zwei Benachrichtigungen versendet, die den Benutzernamen und das initiale Kennwort enthalten. Zur Erzeugung der Benachrichtigungen werden Mailvorlagen genutzt. In einer Mailvorlage sind die Mailtexte in verschiedenen Sprachen definiert. Somit wird bei Generierung einer E-Mail Benachrichtigung die Sprache des Empfängers berücksichtigt. In der Standardinstallation sind bereits Mailvorlagen enthalten, die Sie zur Konfiguration der Benachrichtigungsverfahren verwenden können.

Um Benachrichtigungen über Anmeldeinformationen zu nutzen

1. Stellen Sie sicher, dass das E-Mail-Benachrichtungssystem im One Identity Manager konfiguriert ist. Ausführliche Informationen finden Sie im *One Identity Manager Installationshandbuch*.
2. Aktivieren Sie im Designer den Konfigurationsparameter **Common | MailNotification | DefaultSender** und geben Sie die Absenderadresse an, mit der die E-Mail Benachrichtigungen verschickt werden.
3. Stellen Sie sicher, dass alle Personen eine Standard-E-Mail-Adresse besitzen. An diese E-Mail Adresse werden die Benachrichtigungen versendet. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.
4. Stellen Sie sicher, dass für alle Personen eine Sprachkultur ermittelt werden kann. Nur so erhalten die Personen die E-Mail Benachrichtigungen in ihrer Sprache. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Wenn bei der Neuanlage eines Benutzerkontos ein zufällig generiertes initiales Kennwort vergeben wird, werden die initialen Anmeldeinformationen für dieses Benutzerkonto per E-Mail an eine vorher festgelegt Person gesendet.

Um die initialen Anmeldeinformationen per E-Mail zu versenden

1. Aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\SAPR3\Accounts\InitialRandomPassword".
2. Aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\SAPR3\Accounts\InitialRandomPassword\SendTo" und erfassen Sie als Wert den Empfänger der Benachrichtigung.
3. Aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\SAPR3\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName".

   Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage "Person - Erstellung neues Benutzerkonto" versendet. Die Benachrichtigung enthält den Namen des Benutzerkontos.
4. Aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\SAPR3\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword".

Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage "Person - Initiales Kennwort für neues Benutzerkonto" versendet. Die Benachrichtigung enthält das initiale Kennwort für das Benutzerkonto.

HINWEIS: Um andere als die Standardmailvorlagen für diese Benachrichtigungen zu nutzen, ändern Sie die Werte der Konfigurationsparameter.

5

SAP Systeme

HINWEIS: Die Einrichtung der SAP Systeme in der One Identity Manager-Datenbank übernimmt der Synchronization Editor.

Um die Stammdaten eines SAP Systems zu bearbeiten

1. Wählen Sie die Kategorie **SAP R/3 | Systeme**.
2. Wählen Sie in der Ergebnisliste das SAP System aus und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten des Systems.
4. Speichern Sie die Änderungen.

Tabelle 40: Stammdaten eines SAP Systems

Eigenschaft	Beschreibung
Anzeigename	Anzeigename des SAP Systems.
Systemnummer	Systemnummer des SAP Systems.
Systemvermessung aktiviert	Angabe, ob für dieses System Systemvermessungen durchgeführt werden. Der One Identity Manager stellt die Vermessungsdaten zur Verfügung, die eigentliche Systemvermessung erfolgt jedoch in der SAP R/3-Umgebung.

Verwandte Themen

- Bereitstellen der Daten für die Systemvermessung auf Seite 210

SAP Mandanten

HINWEIS: Die Einrichtung der Mandanten in der One Identity Manager-Datenbank übernimmt der Synchronization Editor.

Um die Stammdaten eines Mandanten zu bearbeiten

1. Wählen Sie die Kategorie **SAP R/3 | Mandanten**.
2. Wählen Sie in der Ergebnisliste den Mandanten. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Bearbeiten Sie die Stammdaten des Mandanten.
4. Speichern Sie die Änderungen.

Allgemeine Stammdaten eines SAP Mandanten

Auf dem Tabreiter **Allgemein** erfassen Sie folgende allgemeinen Stammdaten.

Tabelle 41: Allgemeine Stammdaten eines Mandanten

Eigenschaft	Beschreibung
Mandantennummer	Nummer des Mandanten.
Bezeichnung	Bezeichnung des Mandanten.
System	System, zu dem der Mandant gehört.
Kanonischer Name	Kanonischer Name des Mandanten.
Firma	Firma, für die der Mandant eingerichtet ist. Die hier angegebene Firma wird beim Einrichten neuer Benutzerkonten verwendet.
Ort	Ort der Firma.

Eigenschaft	Beschreibung
Hat Benutzerverwaltung	Angabe, ob der Mandant für die Benutzerverwaltung genutzt wird. Wenn die Option aktiviert ist, kann die höchstwertige Lizenz der Benutzerkonten für die Systemvermessung ermittelt werden.
Kontendefinition (initial)	Initiale Kontendefinition zur Erzeugung von Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für diesen Mandanten die automatische Zuordnung von Personen zu Benutzerkonten genutzt wird und dabei bereits verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen sollen. Es wird der Standardautomatisierungsgrad der Kontendefinition angewendet. Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen Synchronisation der Fall. HINWEIS: Wenn für diesen Mandanten der ZBV Status **Tochtersystem** zugeordnet ist, sollte keine Kontendefinition zugeordnet werden.
Zielsystemverantwortliche	Anwendungsrolle, in der die Zielsystemverantwortlichen des Mandanten festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte des Mandanten, dem sie zugeordnet sind. Jedem Mandanten können andere Zielsystemverantwortliche zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle aus, deren Mitglieder verantwortlich für die Administration dieses Mandanten sind. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.
Synchronisiert durch	HINWEIS: Die Art der Synchronisation können Sie nur festlegen, wenn Sie einen Mandanten neu anlegen. Nach dem Speichern sind keine Änderungen möglich. Beim Erstellen eines Mandaten mit dem Synchronization Editor wird **One Identity Manager** verwendet. Art der Synchronisation, über welche die Daten zwischen dem Mandanten und dem One Identity Manager ausgetauscht werden. Sobald Objekte für diesen Mandanten im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden. Beim Erstellen eines Mandanten mit dem Synchronization Editor wird **One Identity Manager** verwendet.

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td></td><td>
Tabelle 42: Zulässige Werte
<table>
<tr><th>Wert</th><th>Synchronisation durch</th><th>Provisionierung durch</th></tr>
<tr><td>One Identity Manager</td><td>SAP R/3 Konnektor</td><td>SAP R/3 Konnektor</td></tr>
<tr><td>Keine Synchro-nisation</td><td>keine</td><td>keine</td></tr>
</table>
HINWEIS: Wenn Sie Keine Synchronisation festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.
</td></tr>
<tr><td>ALE Name</td><td>Name, mit dem der Mandant als logisches System im SAP-Verteilungsmodell abgebildet ist.</td></tr>
<tr><td>ALE Modellname</td><td>Name des SAP-Verteilungsmodells, das die Beziehungen zwischen den logischen Systemen der Zentralen Benut-zerverwaltung abbildet. Bei der Synchronisation eines Zentralsystems werden die SAP Rollen und Profile aller Tochtersysteme synchronisiert, die den selben ALE Modell-namen haben, wie das Zentralsystem.</td></tr>
<tr><td>ZBV Status</td><td>Verwendung des Mandanten, wenn die Zentrale Benut-zerverwaltung genutzt wird. Mögliche Werte sind Zentralsystem und Tochtersystem.
Der Wert kein ZBV-System zeigt an, dass der Mandant nicht in einer Zentralen Benutzerverwaltung genutzt wird.</td></tr>
<tr><td>Zentralsystem der ZBV</td><td>Zentralsystem, zu dem dieser Mandant gehört. Für Mandanten mit dem ZBV Status Tochtersystem ordnen Sie das gültige Zentralsystem zu.</td></tr>
<tr><td>Beschreibung</td><td>Freitextfeld für zusätzliche Erläuterungen.</td></tr>
</table>

Verwandte Themen

- Einrichten von Kontendefinitionen auf Seite 66
- Zuweisen der Kontendefinition an ein Zielsystem auf Seite 82
- Zielsystemverantwortliche auf Seite 90
- Besonderheiten bei der Synchronisation mit dem Zentralsystem einer ZBV auf Seite 35
- Tochtersystem von der Synchronisation ausschließen auf Seite 36
- Bereitstellen der Daten für die Systemvermessung auf Seite 210

Festlegen der Kategorien für die Vererbung von SAP Gruppen, SAP Rollen und SAP Profilen

HINWEIS: Für ein leichteres Verständnis ist in diesem Abschnitt das Verhalten anhand der SAP Gruppen beschrieben. Es gilt gleichermaßen für Rollen und Profile.

Im One Identity Manager können Gruppen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält verschiedene Tabellen. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In den übrigen Tabellen geben Sie Ihre Kategorien für die zielsystemabhängigen Gruppen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 31**.

HINWEIS: Wenn eine Zentrale Benutzerverwaltung eingesetzt wird, definieren Sie die Kategorien sowohl am Zentralsystem als auch an den Tochtersystemen. Damit Gruppen aus einem Tochtersystem an Benutzerkonten vererbt werden können, müssen an den Tochtersystemen die selben Kategorien definiert sein wie am Zentralsystem.

Um Kategorien zu definieren

1. Wählen Sie im Manager in der Kategorie **SAP R/3 | Mandanten** den Mandanten.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wechseln Sie auf den Tabreiter **Abbildungsvorschrift Kategorien**.
4. Erweitern Sie den jeweiligen Basisknoten einer Tabelle.
5. Aktivieren Sie die Kategorie per Maus-Doppelklick auf das Symbol .
6. Tragen Sie eine beliebige Benennung der Kategorie für Benutzerkonten und Gruppen in der verwendeten Anmeldesprache ein.
7. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Vererbung von SAP Gruppen, SAP Rollen und SAP Profilen anhand von Kategorien auf Seite 188
- One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul

Synchronisationsprojekt bearbeiten

Synchronisationsprojekte, in denen ein Mandant bereits als Basisobjekt verwendet wird, können auch über den Manager geöffnet werden. In diesem Modus können beispielsweise

die Konfigurationseinstellungen überprüft oder die Synchronisationsprotokolle eingesehen werden. Der Synchronization Editor wird nicht mit seinem vollen Funktionsumfang gestartet. Verschiedene Funktionen, wie Simulieren oder Ausführen einer Synchronisation, Starten des Zielsystembrowsers und andere, können nicht ausgeführt werden.

HINWEIS: Der Manager ist währenddessen für die Bearbeitung gesperrt. Um Objekte im Manager bearbeiten zu können, schließen Sie den Synchronization Editor.

Um ein bestehendes Synchronisationsprojekt im Synchronization Editor zu öffnen

1. Wählen Sie die Kategorie **SAP R/3 | Mandanten**.
2. Wählen Sie in der Ergebnisliste den Mandanten. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten...**.

Detaillierte Informationen zum Thema

- One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation

Verwandte Themen

- Anpassen einer Synchronisationskonfiguration auf Seite 39

SAP Benutzerkonten

Mit dem One Identity Manager können Sie die Benutzerkonten einer SAP R/3-Umgebung verwalten. Dabei konzentriert sich der One Identity Manager auf die Einrichtung und Bearbeitung von SAP Benutzerkonten. Um den SAP Benutzerkonten die benötigten Berechtigungen zur Verfügung zu stellen, werden im One Identity Manager Gruppen, Rollen und Profile abgebildet. Zusätzlich werden die benötigten Daten zur Systemvermessung abgebildet. Im One Identity Manager werden die Daten zur Systemvermessung zur Verfügung gestellt, die eigentliche Vermessung erfolgt jedoch in der SAP R/3-Umgebung.

Werden Benutzerkonten in der SAP R/3-Umgebung über die Zentrale Benutzerverwaltung (ZBV) administriert, kann den Benutzerkonten im One Identity Manager der Zugriff auf die Tochtersysteme gewährt und entzogen werden.

Detaillierte Informationen zum Thema

- Benutzerkonten mit Personen verbinden auf Seite 127
- Unterstützte Typen von Benutzerkonten auf Seite 128
- Erfassen der Stammdaten für SAP Benutzerkonten auf Seite 135

Benutzerkonten mit Personen verbinden

Zentraler Bestandteil des One Identity Manager ist die Abbildung von Personen mit ihren Stammdaten sowie den Berechtigungen, über die sie in verschiedenen Zielsystemen verfügen. Zu diesem Zweck können Informationen über Benutzerkonten und Berechtigungen aus den Zielsystemen in die One Identity Manager-Datenbank eingelesen und mit den Personen verbunden werden. Für jede Person kann damit ein Überblick über ihre Berechtigungen in allen angebundenen Zielsystemen gewonnen werden. Der One Identity Manager bietet die Möglichkeit Benutzerkonten und ihre Berechtigungen zu verwalten. Änderungen können in die Zielsysteme provisioniert werden. Die Personen werden so entsprechend ihrer Funktion mit den benötigten Berechtigungen in den angebundenen Zielsystemen versorgt. Regelmäßige Synchronisationsprozesse halten die Daten zwischen den Zielsystemen und der One Identity Manager-Datenbank konsistent.

Da die Anforderungen von Unternehmen zu Unternehmen unterschiedlich sind, bietet der One Identity Manager verschiedene Verfahren zur Versorgung einer Person mit den benötigten Benutzerkonten an. Der One Identity Manager unterstützt die folgenden Vorgehensweisen, um Personen und ihre Benutzerkonten zu verknüpfen:

- Personen erhalten ihre Benutzerkonten automatisch über Kontendefinitionen. Hat eine Person noch kein Benutzerkonto in einem Mandanten, wird durch die Zuweisung der Kontendefinition an eine Person über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

  Wenn Sie Benutzerkonten über Kontendefinitionen verwalten, können Sie das Verhalten von Benutzerkonten beim Deaktivieren oder Löschen von Personen festlegen.
- Beim Einfügen eines Benutzerkontos wird automatisch eine vorhandene Person zugeordnet oder im Bedarfsfall eine neue Person erstellt. Dabei werden die Personenstammdaten anhand vorhandener Benutzerkontenstammdaten erzeugt. Dieser Mechanismus kann eingesetzt werden, wenn ein neues Benutzerkonto manuell oder durch eine Synchronisation erstellt wird. Dieses Vorgehen ist jedoch nicht das Standardverfahren für den One Identity Manager. Für die automatische Personenzuordnung definieren Sie Kriterien, anhand derer die Personen ermittelt werden sollen.
- Personen und Benutzerkonten können manuell erfasst und einander zugeordnet werden.

Verwandte Themen

- Erfassen der Stammdaten für SAP Benutzerkonten auf Seite 135
- Einrichten von Kontendefinitionen auf Seite 66
- Automatische Zuordnung von Personen zu SAP Benutzerkonten auf Seite 156

Ausführliche Informationen zu den Grundlagen zur Behandlung und Administration von Personen und Benutzerkonten finden Sie im One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

Unterstützte Typen von Benutzerkonten

Im One Identity Manager können unterschiedliche Typen von Benutzerkonten wie beispielsweise Standardbenutzerkonten, administrative Benutzerkonten, Dienstkonten oder privilegierte Benutzerkonten abgebildet werden.

Zur Abbildung der verschiedenen Benutzerkontentypen werden die folgenden Eigenschaften verwendet.

- Identität

  Mit der Eigenschaft **Identität** (Spalte `IdentityType`) wird der Typ des Benutzerkontos beschrieben.

Tabelle 43: Identitäten von Benutzerkonten

Identität	Beschreibung	Wert der Spalte IdentityType
Primäre Identität	Standardbenutzerkonto einer Person.	Primary
Organisatorische Identität	Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen.	Organizational
Persönliche Administratoridentität	Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird.	Admin
Zusatzidentität	Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird.	Sponsored
Gruppenidentität	Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird.	Shared
Dienstidentität	Dienstkonto.	Service

HINWEIS: Um mit Identitäten für Benutzerkonten zu arbeiten, benötigen die Personen ebenfalls Identitäten. Benutzerkonten, denen eine Identität zugeordnet ist, können Sie nur mit Personen verbinden, die dieselbe Identität haben.

Die primäre Identität, die organisatorische Identität und die persönliche Administratoridentität werden für die verschiedenen Benutzerkonten genutzt, mit denen ein und dieselbe Person ihre unterschiedlichen Aufgaben im Unternehmen ausführen kann.

Um Benutzerkonten mit einer persönlichen Administratoridentität oder einer organisatorische Identität für eine Person bereitzustellen, richten Sie für die Person Subidentitäten ein. Diese Subidentitäten verbinden Sie mit den Benutzerkonten. Somit können für die unterschiedlichen Benutzerkonten die erforderlichen Berechtigungen erteilt werden.

Benutzerkonten mit einer Zusatzidentität, einer Gruppenidentität oder einer Dienstidentität verbinden Sie mit Dummy-Personen, die keinen Bezug zu einer realen Person haben. Diese Dummy-Personen werden benötigt, um Berechtigungen an die Benutzerkonten vererben zu können. Bei der Auswertung von Berichten, Attestierungen oder Complianceprüfungen prüfen Sie, ob die Dummy-Personen gesondert betrachtet werden müssen.

Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

- Privilegiertes Benutzerkonto

Privilegierte Benutzerkonten werden eingesetzt, um Personen mit zusätzlichen privilegierten Berechtigungen auszustatten. Dazu gehören beispielsweise administrative Benutzerkonten oder Dienstkonten. Die Benutzerkonten werden mit der Eigenschaft **Privilegiertes Benutzerkonto** (Spalte `IsPrivilegedAccount`) gekennzeichnet.

Standardbenutzerkonten

In der Regel erhält jede Person ein Standardbenutzerkonto, das die Berechtigungen besitzt, die für die tägliche Arbeit benötigt werden. Die Benutzerkonten haben eine Verbindung zur Person. Über eine Kontendefinition und deren Automatisierungsgrade kann die Auswirkung der Verbindung und der Umfang der vererbten Eigenschaften der Person an die Benutzerkonten konfiguriert werden.

Um Standardbenutzerkonten über Kontendefinitionen zu erstellen

1. Erstellen Sie eine Kontendefinition und weisen Sie die Automatisierungsgrade **Unmanaged** und **Full managed** zu.
2. Legen Sie für jeden Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll.
3. Erstellen Sie eine Abbildungsvorschrift für die IT Betriebsdaten.

   Mit der Abbildungsvorschrift legen Sie fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über primären Rollen einer Person ermittelt werden können.

   Welche IT Betriebsdaten erforderlich sind, ist abhängig vom Zielsystem. Für Standardbenutzerkonten werden folgende Einstellungen empfohlen:

   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IsGroupAccount` den Standardwert **1** und aktivieren Sie die Option **Immer Standardwert verwenden**.
   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IdentityType` den Standardwert **Primary** und aktivieren Sie die Option **Immer Standardwert verwenden**.
4. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem. Wählen Sie unter **Wirksam für** das konkrete Zielsystem.

   Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.
5. Weisen Sie die Kontendefinition an die Personen zu.

   Durch die Zuweisung der Kontendefinition an eine Person wird über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

Administrative Benutzerkonten

Für bestimmte administrative Aufgaben, ist der Einsatz administrativer Benutzerkonten notwendig. Administrative Benutzerkonten werden in der Regel vom Zielsystem vorgegeben und haben feste Bezeichnungen und Anmeldenamen, wie beispielsweise **Administrator**.

Administrative Benutzerkonten werden durch die Synchronisation in den One Identity Manager eingelesen.

HINWEIS: Einige administrative Benutzerkonten können automatisch als privilegierte Benutzerkonten gekennzeichnet werden. Aktivieren Sie dazu im Designer den Zeitplan **Ausgewählte Benutzerkonten als privilegiert kennzeichnen**.

Administrative Benutzerkonten können Sie als **Persönliche Administratoridentität** oder als **Gruppenidentität** kennzeichnen. Um die Personen, welche diese Benutzerkonten nutzen, mit den benötigten Berechtigungen zu versorgen, gehen Sie folgendermaßen vor.

- Persönliche Administratoridentität
  1. Verbinden Sie das Benutzerkonto über die Spalte `UID_Person` mit einer Person.

     Nutzen Sie eine Person mit derselben Identität oder erstellen Sie eine neue Person.
  2. Weisen Sie diese Person an hierarchische Rollen zu.
- Gruppenidentität
  1. Weisen Sie dem Benutzerkonto alle Personen mit Nutzungsberechtigungen zu.
  2. Verbinden Sie das Benutzerkonto über die Spalte `UID_Person` mit einer Dummy-Person.

     Nutzen Sie eine Person mit derselben Identität oder erstellen Sie eine neue Person.
  3. Weisen Sie diese Dummy-Person an hierarchische Rollen zu.

  Das Benutzerkonto erhält seine Berechtigungen über die Dummy-Person.

Privilegierte Benutzerkonten

Privilegierte Benutzerkonten werden eingesetzt, um Personen mit zusätzlichen privilegierten Berechtigungen auszustatten. Dazu gehören beispielsweise administrative Benutzerkonten oder Dienstkonten. Die Benutzerkonten werden mit der Eigenschaft **Privilegiertes Benutzerkonto** (Spalte `IsPrivilegedAccount`) gekennzeichnet.

HINWEIS: Die Kriterien anhand derer Benutzerkonten automatisch als privilegiert erkannt werden, sind als Erweiterungen zur Sichtdefinition (ViewAddOn) an der Tabelle `TSBVAccountIsPrivDetectRule` (Tabelle vom Typ **Union**) definiert. Die Auswertung erfolgt im Skript `TSB_SetIsPrivilegedAccount`.

Um privilegierte Benutzerkonten über Kontendefinitionen zu erstellen

1. Erstellen Sie eine Kontendefinition. Erstellen Sie einen neuen Automatisierungsgrad für privilegierte Benutzerkonten und weisen Sie diesen Automatisierungsgrad an die

Kontendefinition zu.

2. Wenn Sie verhindern möchten, dass die Eigenschaften für privilegierte Benutzerkonten überschrieben werden, setzen Sie für den Automatisierungsgrad die Eigenschaft **IT Betriebsdaten überschreibend** auf den Wert **Nur initial**. In diesem Fall werden die Eigenschaften einmalig beim Erstellen der Benutzerkonten befüllt.
3. Legen Sie für den Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll.
4. Erstellen Sie eine Abbildungsvorschrift für die IT Betriebsdaten.

   Mit der Abbildungsvorschrift legen Sie fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden, und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über primären Rollen einer Person ermittelt werden können.

   Welche IT Betriebsdaten erforderlich sind, ist abhängig vom Zielsystem. Für privilegierte Benutzerkonten werden folgende Einstellungen empfohlen:

   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IsPrivilegedAccount` den Standardwert **1** und aktivieren Sie die Option **Immer Standardwert verwenden**.
   - Zusätzlich können Sie eine Abbildungsvorschrift für die Spalte `IdentityType` festlegen. Die Spalte besitzt verschiedene zulässige Werte, die privilegierte Benutzerkonten repräsentieren.
   - Um zu verhindern, das privilegierte Benutzerkonten die Berechtigungen des Standardbenutzers erben, definieren Sie eine Abbildungsvorschrift für die Spalte `IsGroupAccount` mit dem Standardwert **0** und aktivieren Sie die Option **Immer Standardwert verwenden**.
5. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem.

   Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.
6. Weisen Sie die Kontendefinition direkt an die Personen zu, die mit privilegierten Benutzerkonten arbeiten sollen.

   Durch die Zuweisung der Kontendefinition an eine Person wird über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

TIPP: Wenn es unternehmensspezifisch erforderlich ist, dass die Anmeldenamen privilegierter Benutzerkonten einem definierten Namensschema folgen, legen Sie die Bildungsregel fest, nach der die Anmeldenamen gebildet werden.

Zentrale Benutzerverwaltung im One Identity Manager

Werden Benutzerkonten in der SAP R/3-Umgebung über die Zentrale Benutzerverwaltung (ZBV) administriert, kann den Benutzerkonten im One Identity Manager der Zugriff auf die Tochtersysteme gewährt und entzogen werden. Dafür werden die Mandanten im One Identity Manager als Zentralsystem oder Tochtersystem gekennzeichnet. Die Benutzerkonten werden im Zentralsystem verwaltet. Für jedes Benutzerkonto legen Sie fest, in welchen Mandanten es Zugriffsberechtigungen erhalten darf (Tabelle SAPUserMandant). Einem Benutzerkonto können nur SAP Gruppen, Rollen oder Profile aus diesen Mandanten zugewiesen werden. Über Zugriffsberechtigungen im Zentralsystem verfügt ein Benutzerkonto nur, wenn auch das Zentralsystem in der Tabelle SAPUserMandant explizit zugewiesen ist.

Um die automatische Personenzuordnung für die Benutzerkonten einer Zentralen Benutzerverwaltung (ZBV) zu nutzen, weisen Sie dem Zentralsystem der ZBV eine Kontendefinition mit der Benutzerkontentabelle **SAPUser** zu.

Die Zugriffsberechtigungen für Zentral- und Tochtersysteme werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Im One Identity Manager kann die Zugriffsberechtigung sowohl über IT Shop-Bestellungen und indirekte Zuweisung als auch über Direktzuweisung gewährt werden.

Um einer Person den Zugriff auf einen Mandanten durch indirekte Zuweisung oder Bestellung zu gewähren

1. Erstellen Sie eine Kontendefinition zum Erzeugen von Benutzerkonten im Zentralsystem.

   Wählen Sie im Eingabefeld **Benutzerkontentabelle** die Tabelle **SAPUser**. Weitere Informationen finden Sie unter Stammdaten einer Kontendefinition auf Seite 67.

   Diese Kontendefinition wird benötigt, um ein Benutzerkonto im Zentralsystem zu erzeugen, falls die Person noch kein Benutzerkonto besitzt.

2. Erstellen Sie eine Kontendefinition für den Mandanten, für den der Zugriff gewährt werden soll. Es gelten folgende Besonderheiten:

   Tabelle 44: Stammdaten einer Kontendefinition für den Zugriff auf Mandanten

Eigenschaft	Beschreibung
Benutzerkontentabelle	Wählen Sie aus der Auswahlliste **SAPUserMandant**.
Zielsystem	Mandant, für den der Zugriff gewährt werden soll.
Vorausgesetzte Kontendefinition	Wählen Sie aus der Auswahlliste die Kontendefinition zum Erzeugen von Benutzerkonten im Zentralsystem. Damit wird ein Benutzerkonto im Zentralsystem erzeugt, falls die

Eigenschaft	Beschreibung
	Person noch kein Benutzerkonto hat.
Automatisierungsgrad (initial)	Wählen Sie aus der Auswahlliste **Unmanaged**.
Leistungsposition	Leistungsposition, über welche die Kontendefinition im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.
IT Shop	Aktivieren Sie die Option, wenn der Zugriff auf das Tochtersystem im Web Portal bestellt werden darf.
Verwendung nur im IT Shop	Aktivieren Sie die Option, wenn der Zugriff auf das Tochtersystem ausschließlich im Web Portal bestellt werden soll. Eine indirekte Zuweisung über Geschäftsrollen oder Organisationen ist nicht möglich. Der Zugriff eines Benutzerkontos auf das Tochtersystem kann aber noch direkt gewährt werden.

   Es wird je eine Kontendefinition für jedes Tochtersystem und für das Zentralsystem benötigt, in denen der Zugriff gewährt werden soll.

3. Weisen Sie die Kontendefinition für den Mandanten an eine hierarchische Rolle oder ein IT Shop Regal zu.
4. Nehmen Sie die Person als Mitglied in die hierarchische Rolle oder als Kunde in den IT Shop auf.

Um einem Benutzerkonto den Zugriff auf einen Mandanten direkt zu gewähren

- Weisen Sie dem Benutzerkonto alle Mandanten zu, in denen es Zugriffsberechtigungen erhalten darf.

  Weitere Informationen finden Sie unter Zugriff auf Mandaten einer Zentralen Benutzerverwaltung gewähren auf Seite 151.

Dem Benutzerkonto können nun die SAP Gruppen, Rollen, Profile aus diesen Mandanten zugewiesen werden.

Detaillierte Informationen zum Thema

- Einrichten von Kontendefinitionen auf Seite 66

Verwandte Themen

- Allgemeine Stammdaten eines SAP Mandanten auf Seite 122
- SAP Gruppen, SAP Rollen und SAP Profile an SAP Benutzerkonten zuweisen auf Seite 173
- Automatische Zuordnung von Personen zu SAP Benutzerkonten auf Seite 156

Erfassen der Stammdaten für SAP Benutzerkonten

Ein Benutzerkonto kann im One Identity Manager mit einer Person verbunden sein. Ebenso können Sie die Benutzerkonten getrennt von Personen verwalten.

HINWEIS: Um Benutzerkonten für die Personen eines Unternehmens einzurichten, wird der Einsatz von Kontendefinitionen empfohlen. Einige der nachfolgend beschriebenen Stammdaten werden dabei über Bildungsregeln aus den Personenstammdaten gebildet.

HINWEIS:Sollen Personen ihre Benutzerkonten über Kontendefinitionen erhalten, müssen die Personen ein zentrales Benutzerkonto besitzen und über die Zuordnung zu einer primären Abteilung, einem primären Standort oder einer primären Kostenstelle ihre IT Betriebsdaten erhalten.Sollen Personen ihre Benutzerkonten über Kontendefinitionen erhalten, müssen die Personen ein zentrales SAP Benutzerkonto besitzen und über die Zuordnung zu einer primären Abteilung, einem primären Standort oder einer primären Kostenstelle ihre IT Betriebsdaten erhalten.

Um ein Benutzerkonto zu erstellen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Benutzerkonten**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

Um die Stammdaten eines Benutzerkontos zu bearbeiten

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

Um ein Benutzerkonto für eine Person manuell zuzuweisen oder zu erstellen

1. Wählen Sie im Manager die Kategorie **Personen | Personen**.
2. Wählen Sie in der Ergebnisliste die Person und führen Sie die Aufgabe **SAP Benutzerkonten zuweisen** aus.
3. Weisen Sie ein Benutzerkonto zu.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines SAP Benutzerkontos auf Seite 136
- Logondaten eines SAP Benutzerkontos auf Seite 140

- Telefonnummern auf Seite 142
- Faxnummern auf Seite 143
- E-Mail-Adressen auf Seite 144
- SAP Parameter direkt zuweisen auf Seite 146
- Festwerte eines SAP Benutzerkontos auf Seite 145
- Vermessungsdaten auf Seite 145
- SNC-Daten eines SAP Benutzerkontos auf Seite 146

Allgemeine Stammdaten eines SAP Benutzerkontos

Tabelle 45: Konfigurationsparameter für die Risikobewertung von SAP Benutzerkonten

Konfigurationsparameter	Wirkung bei Aktivierung
QER\CalculateRiskIndex	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Berechnung des Risikoindex. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Werte für den Risikoindex erfasst und berechnet werden.

HINWEIS: Werden Benutzerkonten im SAP System über eine Zentrale Benutzerverwaltung administriert, können Sie Benutzerkonten nur in Mandanten, die als Zentralsystem gekennzeichnet sind, anlegen.

Die allgemeinen Stammdaten eines Benutzerkontos erfassen Sie auf dem Tabreiter **Adresse**.

Tabelle 46: Adressdaten eines SAP Benutzerkontos

Eigenschaft	Beschreibung
Person	Person, die das Benutzerkonto verwendet. Wurde das Benutzerkonto über eine Kontendefinition erzeugt, ist die Person bereits eingetragen. Wenn Sie das Benutzerkonto manuell erstellen, können Sie die Person aus der Auswahlliste wählen.Wenn Sie die automatische Personenzuordnung nutzen, wird beim Speichern des Benutzerkontos eine zugehörige Person gesucht und in das Benutzerkonto übernommen. Für ein Benutzerkonto mit einer Identität vom Typ **Organisatorische Identität**, **Persönliche Administratoridentität**, **Zusatzidentität**, **Gruppenidentität**

Eigenschaft	Beschreibung
	oder **Dienstidentität** können Sie eine neue Person erstellen. Klicken Sie dafür neben dem Eingabefeld und erfassen Sie die erforderlichen Personenstammdaten. Die Pflichteingaben sind abhängig vom gewählten Identitätstyp.
Kontendefinition	Kontendefinition, über die das Benutzerkonto erstellt wurde. Die Kontendefinition wird benutzt, um die Stammdaten des Benutzerkontos automatisch zu befüllen und um einen Automatisierungsgrad für das Benutzerkonto festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Person und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein. HINWEIS: Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden.
Automatisierungsgrad	Automatisierungsgrad des Benutzerkontos. Wählen Sie einen Automatisierungsgrad aus der Auswahlliste. Den Automatisierungsgrad können Sie nur festlegen, wenn Sie auch eine Kontendefinition eingetragen haben. In der Auswahlliste werden alle Automatisierungsgrade der gewählten Kontendefinition angeboten.
Mandant	Mandant, in dem das Benutzerkonto angelegt werden soll. Zentralsystem, wenn die Benutzerkonten über eine ZBV administriert werden. Den Mandanten können Sie nur bearbeiten, wenn Sie ein neues Benutzerkonto anlegen.
Benutzerkonto	Bezeichnung des Benutzerkontos. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. HINWEIS:Bestehende Benutzerkonten können nicht umbenannt werden.
Vorname	Vorname des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Nachname	Nachname des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Anrede	Anrede in der Anmeldesprache des zugehörigen Mandanten. Wenn Sie eine Kontendefinition zugeordnet haben, wird die Anrede abhängig vom Automatisierungsgrad über eine Bildungsregel ermittelt. Die Anrede ist abhängig vom Geschlecht der zugeordneten Person.

Eigenschaft	Beschreibung
Akademischer Titel	Zusätzliche Information zum Benutzerkonto.
Alias	Alternative Kennung des Benutzerkontos, der zur Anmeldung bei bestimmten Internettransaktionen verwendet wird.
Nickname	Zusätzliche Information zum Benutzerkonto.
Format für Namensaufbereitung	Format und Land für die Namensaufbereitung. Das Format für die Namensaufbereitung und das Land für die Namensaufbereitung bestimmen die Aufbereitungsregeln für die Zusammensetzung eines vollständigen Personennamens in der SAP R/3-Umgebung. Das Namensaufbereitungsformat legt fest, in welcher Reihenfolge welche Namensteile gesammelt werden sollen, um den Namen einer Person in einer ausführlichen Langform darzustellen. Das Land dient zur eindeutigen Identifizierung einer Aufbereitungsregel.
Land für Namensaufbereitung	
ISO 639 - Sprache	Standardsprache des Benutzerkontos nach ISO 639.
Funktion	Zusätzliche Information zum Benutzerkonto. Wird beim Drucken von Adressen berücksichtigt.
Personennummer	SAP-interner Schlüssel zur Identifikation einer Person.
Abteilung	Zusätzliche Information zum Benutzerkonto. Wird beim Drucken von Adressen berücksichtigt.
Raum im Gebäude	Zusätzliche Information zum Benutzerkonto.
Etage	Zusätzliche Information zum Benutzerkonto.
Gebäude (Nummer oder Kürzel)	Zusätzliche Information zum Benutzerkonto.
Kommunikationsart	Eindeutige Kennung der Kommunikationsart.
Firma	Firma, der das Benutzerkonto zugeordnet ist. Bei Neuanlage eines Benutzerkontos wird die Firma des zugeordneten Mandanten zugeordnet. Ist dem Mandanten keine Firma zugeordnet, so wird innerhalb dieses Mandanten die Firma mit der kleinsten Adressnummer ermittelt und dem Benutzerkonto zugeordnet. HINWEIS: **Firma** ist ein Pflichtfeld! Änderungen an Benutzerkonten, denen im SAP R/3-System keine Firma zugeordnet ist, können bei der Synchronisation im One Identity Manager nicht gespeichert werden. Ordnen Sie diesen Benutzerkonten im SAP R/3-System nach Möglichkeit eine Standardfirma zu.
Risikoindex	Maximalwert der Risikoindexwerte aller zugeordneten Gruppen,

Eigenschaft	Beschreibung
(berechnet)	Rollen und Profile. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen, Rollen und Profilen an das Benutzerkonto. Gruppen, Rollen und Profilen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen, Rollen und Profilen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Identität	Typ der Identität des Benutzerkontos. Zulässige Werte sind: • **Primäre Identität**: Standardbenutzerkonto einer Person. • **Organisatorische Identität**: Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen. • **Persönliche Administratoridentität**: Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird. • **Zusatzidentität**: Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird. • **Gruppenidentität**: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird. Weisen Sie alle Personen zu, die das Benutzerkonto nutzen. • **Dienstidentität**: Dienstkonto.
Privilegiertes Benutzerkonto	Angabe, ob es sich um ein privilegiertes Benutzerkonto handelt.
Gruppen erbbar	Angabe, ob das Benutzerkonto Gruppen, Rollen und Profile über die Person erben darf. Ist die Option aktiviert, werden Gruppen, Rollen und Profile über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Person eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Gruppe nur, wenn die Option aktiviert ist.

Verwandte Themen

- Benutzerkonten mit Personen verbinden auf Seite 127
- Unterstützte Typen von Benutzerkonten auf Seite 128
- Einrichten von Kontendefinitionen auf Seite 66
- Festlegen der Kategorien für die Vererbung von SAP Gruppen, SAP Rollen und SAP Profilen auf Seite 125
- Allgemeine Stammdaten eines SAP Mandanten auf Seite 122
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul
- One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul
- One Identity Manager Administrationshandbuch für Risikobewertungen

Logondaten eines SAP Benutzerkontos

Beim Einfügen eines neuen Benutzerkontos vergeben Sie ein Kennwort. Nach dem Speichern des Benutzerkontos kann das Kennwort über den Manager nicht mehr geändert werden.

Auf dem Tabreiter **Logondaten** erfassen Sie folgende Daten.

Tabelle 47: Logondaten eines SAP Benutzerkontos

Eigenschaft	Beschreibung
Kennwort	Kennwort für das Benutzerkonto. Das zentrale Kennwort der zugeordneten Person kann auf das Kennwort des Benutzerkontos abgebildet werden. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*. Wenn Sie ein initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen. HINWEIS: Beim Prüfen eines Benutzerkennwortes werden die One Identity Manager Kennwortrichtlinien beachtet. Stellen Sie sicher, dass die Kennwortrichtlinie nicht gegen die Anforderungen des Zielsystems verstößt.
Kennwortbestätigung	Kennwortwiederholung.
Produktivkennwort soll gesetzt werden	Angabe, ob bei Änderung des Kennworts im Zielsystem der Kennwortstatus "Produktivkennwort" gesetzt werden soll.
Deaktiviertes	Angabe, ob das Kennwort deaktiviert ist (wenn Single-Sign-On zu

Eigenschaft	Beschreibung
Kennwort	Anmeldung genutzt wird).
Sicherheitsrichtlinie	Sicherheitsrichtlinie, die für dieses Benutzerkonto gilt.
Benutzergruppe	SAP Gruppe, die als Benutzergruppe für die Berechtigungsprüfung genutzt wird.
Referenzbenutzer	Referenzbenutzer, dessen Berechtigungen das Benutzerkonto zusätzlich erhält. Ein Referenzbenutzer ist ein Benutzerkonto mit dem Benutzertyp "Referenz". Über Referenzbenutzer können Sie identische Berechtigungen an verschiedene Benutzerkonten innerhalb eines Mandanten vergeben.
Benutzerkonto gültig von	Gültigkeitszeitraum des SAP Benutzerkontos.
Benutzerkonto gültig bis	
Abrechnungsnummer	Abrechnungsnummer für die Abrechnung des Benutzerkontos.
Kostenstelle	Kostenstelle für die Abrechnung des Benutzerkontos.
Benutzerkontentyp	Typ des Benutzerkontos. Der Standardwert des Benutzerkontentyps ist im Konfigurationsparameter "TargetSystem\SAPR3\Accounts\Ustyp" festgelegt.
Benutzerkonto gesperrt	Angabe, ob das Benutzerkonto gesperrt ist. Ist das Benutzerkonto mit einer Person verbunden, wird das Benutzerkonto entsperrt, wenn ein neues zentrales Kennwort für die Person gesetzt wird. Das Verhalten wird über den Konfigurationsparameter **TargetSystem | SAPR3 | Accounts | UnlockByCentralPassword** gesteuert. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.
Letzte Anmeldung	Datum und Uhrzeit der letzten Anmeldung am SAP System.

Verwandte Themen

- Kennwortrichtlinien für SAP Benutzerkonten auf Seite 105
- Initiales Kennwort für neue SAP Benutzerkonten auf Seite 116
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 118
- Benutzerkontentypen auf Seite 93
- SAP Benutzerkonto sperren und entsperren auf Seite 154
- Sicherheitsrichtlinien auf Seite 103

Telefonnummern

Auf dem Tabreiter **Telefonnummern** können Sie die Telefonnummern des Benutzerkontos bearbeiten.

Um eine Telefonnummer an ein Benutzerkonto zuzuweisen

1. Wählen Sie den Tabreiter **Telefonnummern**.
2. Klicken Sie **Hinzufügen**.

   Es wird eine neue Zeile in die Tabelle eingefügt.
3. Markieren Sie diese Zeile. Bearbeiten Sie die Stammdaten der Telefonnummer.
4. Speichern Sie die Änderungen.

Um eine Telefonnummer zu bearbeiten

1. Wählen Sie den Tabreiter **Telefonnummern**.
2. Wählen Sie in der Tabelle die Telefonnummer.
3. Bearbeiten Sie die Stammdaten der Telefonnummer.
4. Speichern Sie die Änderungen.

Um die Zuweisung einer Telefonnummer zu entfernen

1. Wählen Sie den Tabreiter **Telefonnummern**.
2. Wählen Sie in der Tabelle die Telefonnummer.
3. Klicken Sie **Entfernen**.
4. Speichern Sie die Änderungen.

Tabelle 48: Eigenschaften einer Telefonnummer

Eigenschaft	Beschreibung
Typ	Typ des Telefonanschlusses. Wählen Sie zwischen "Telefon", "Telefon (Standard)", "Mobiltelefon (Standard)" und "Mobiltelefon".
Land	Land zur Ermittlung der Landesvorwahl.
Telefonnummer	Telefonnummer mit Ortsvorwahl. Um eine Durchwahl zu erfassen, nutzen Sie das zweite Eingabefeld. Wenn Sie eine Kontendefinition zugeordnet haben, wird die Telefonnummer abhängig vom Automatisierungsgrad über eine Bildungsregel ermittelt.
Telefonnummer (komplett)	Vollständige Telefonnummer. Enthält Vorwahl, Anschluss und Durchwahl.
Bevorzugt	Angabe, ob diese Telefonnummer die bevorzugte Telefonnummer des Benutzers ist.

Eigenschaft	Beschreibung
Heimatadresse	Angabe, ob diese Telefonnummer die Heimatnummer des Benutzers ist.
SMS-fähig	Angabe, ob über diese Telefonnummer SMS versendet werden können.

Faxnummern

Auf dem Tabreiter **Faxnummern** können Sie die Faxnummern des Benutzerkontos bearbeiten.

Um eine Faxnummer an ein Benutzerkonto zuzuweisen

1. Wählen Sie den Tabreiter **Faxnummern**.
2. Klicken Sie **Hinzufügen**.

   Es wird eine neue Zeile in die Tabelle eingefügt.
3. Markieren Sie diese Zeile. Bearbeiten Sie die Stammdaten der Faxnummer.
4. Speichern Sie die Änderungen.

Um eine Faxnummer zu bearbeiten

1. Wählen Sie den Tabreiter **Faxnummern**.
2. Wählen Sie in der Tabelle die Faxnummer.
3. Bearbeiten Sie die Stammdaten der Faxnummer.
4. Speichern Sie die Änderungen.

Um die Zuweisung einer Faxnummer zu entfernen

1. Wählen Sie den Tabreiter **Faxnummern**.
2. Wählen Sie in der Tabelle die Faxnummer.
3. Klicken Sie **Entfernen**.
4. Speichern Sie die Änderungen.

Tabelle 49: Faxnummern

Eigenschaft	Beschreibung
Land	Land zur Ermittlung der Landesvorwahl.
FAX-Nummer	Faxnummer mit Ortsvorwahl. Um eine Durchwahl zu erfassen, nutzen Sie das zweite Eingabefeld.
FAX-Nummer (komplett)	Vollständige Faxnummer. Enthält Vorwahl, Anschluss und Durchwahl.
Bevorzugt	Angabe, ob diese Faxnummer die bevorzugte Faxnummer des

Eigenschaft	Beschreibung
	Benutzers ist.
Heimatadresse	Angabe, ob diese Faxnummer die Heimatnummer des Benutzers ist.

E-Mail-Adressen

Auf dem Tabreiter **E-Mail-Adressen** können Sie die E-Mail-Adressen des Benutzerkontos bearbeiten.

Um eine E-Mail-Adresse an ein Benutzerkonto zuzuweisen

1. Wählen Sie den Tabreiter **E-Mail-Adressen**.
2. Klicken Sie **Hinzufügen**.

   Es wird eine neue Zeile in die Tabelle eingefügt.
3. Markieren Sie diese Zeile. Bearbeiten Sie die Stammdaten der E-Mail-Adresse.
4. Speichern Sie die Änderungen.

Um eine E-Mail-Adresse zu bearbeiten

1. Wählen Sie den Tabreiter **E-Mail-Adressen**.
2. Wählen Sie in der Tabelle die E-Mail-Adresse.
3. Bearbeiten Sie die Stammdaten der E-Mail-Adresse.
4. Speichern Sie die Änderungen.

Um die Zuweisung einer E-Mail-Adresse zu entfernen

1. Wählen Sie den Tabreiter **E-Mail-Adressen**.
2. Wählen Sie in der Tabelle die E-Mail-Adresse.
3. Klicken Sie **Entfernen**.
4. Speichern Sie die Änderungen.

Tabelle 50: E-Mail-Adressdaten

Eigenschaft	Beschreibung
E-Mail-Adresse (SMTP)	E-Mail-Adresse.
Suchfeld für die E-Mail-Adresse	Enthält die ersten 20 Zeichen der E-Mail-Adresse in normalisierter Form.
Bevorzugt	Angabe, ob diese E-Mail-Adresse die bevorzugte E-Mail-Adresse des Benutzers ist.
Heimatadresse	Angabe, ob diese E-Mail-Adresse die Heimatadresse des Benutzers ist.

Festwerte eines SAP Benutzerkontos

Tabelle 51: Konfigurationsparameter für die Einrichtung von Benutzerkonten

Konfigurationsparameter	Wirkung bei Aktivierung
TargetSystem\SAPR3\Accounts\Datfm	Festlegung des Standard-Datumsformates für SAP Benutzerkonten.
TargetSystem\SAPR3\Accounts\Dcpfm	Festlegung des Standard-Dezimalpunktformates für SAP Benutzerkonten.
TargetSystem\SAPR3\Accounts\Fax_Group	Festlegung der Standard-Faxgruppe für SAP Benutzerkonten.
TargetSystem\SAPR3\Accounts\Guiflag	Festlegung für SAP Benutzerkonten, ob die unsichere Kommunikation erlaubt ist.
TargetSystem\SAPR3\Accounts\Spda	Festlegung der Standardeinstellung für Druckparameter 3 (Löschen nach Druck).
TargetSystem\SAPR3\Accounts\Spdb	Festlegung der Standardeinstellung für Druckparameter 2 (Drucken sofort).
TargetSystem\SAPR3\Accounts\Splg	Festlegung des Standarddruckers (Druckparameter 1).
TargetSystem\SAPR3\Accounts\Time_zone	Festlegung des Standardwertes für die Zeitzone der Adresse eines SAP Benutzerkontos.
TargetSystem\SAPR3\Accounts\Tzone	Festlegung des Standardwertes für die Zeitzone.

Auf dem Tabreiter **Festwerte** legen Sie allgemeine Einstellungen fest, die für das Benutzerkonto wirksam werden sollen. Diese Angaben umfassen beispielsweise das Startmenü, welches nach Anmeldung angeboten werden soll, die Standard-Anmeldesprache, die persönliche Zeitzone, die Dezimaldarstellung oder das Datumsformat, mit denen der Benutzer arbeitet.

Um Standardwerte für die Festwerte festzulegen

- Bearbeiten Sie im Designer die Werte der Konfigurationsparameter unter "TargetSystem\SAPR3\Accounts".

Vermessungsdaten

Auf dem Tabreiter **Vermessungsdaten** werden die Lizenzangaben für die Systemvermessung abgebildet. Weitere Informationen finden Sie unter Bereitstellen der Daten für die Systemvermessung auf Seite 210.

SNC-Daten eines SAP Benutzerkontos

Auf dem Tabreiter **SNC** erfassen Sie die Daten, die für die Anmeldung am System über Secure Network Communications (SNC) erforderlich sind.

Tabelle 52: SNC-Daten eines Benutzerkontos

Eigenschaften	Beschreibung
SNC Name	SNC Namen des Benutzerkontos. Die Syntax für SNC Namen entnehmen Sie Ihrem SNC Benutzerhandbuch.
Unsichere Kommunikation erlaubt	Angabe, ob für das Benutzerkonto die unsichere Kommunikation erlaubt ist.

SAP Parameter direkt zuweisen

Auf dem Tabreiter **Parameter** können Sie einem Benutzerkonto Parameter direkt zuweisen und deren Werte festlegen. Außerdem sehen Sie hier, ob ein Parameter direkt, indirekt oder über beide Wege zugewiesen ist.

Um einen Parameter an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Wählen Sie den Tabreiter **Parameter**.
4. Klicken Sie **Hinzufügen**.

   Es wird eine neue Zeile in die Tabelle eingefügt.
5. Markieren Sie diese Zeile per Mausklick.
6. Wählen Sie aus der Auswahlliste **Parameter** einen Parameter und legen Sie den Parameterwert fest.
7. Speichern Sie die Änderungen.

Um einen Parameterwert zu bearbeiten

1. Wählen Sie den Tabreiter **Parameter**.
2. Wählen Sie in der Tabelle den Parameter, dessen Wert Sie ändern möchten.
3. Ändern Sie den Parameterwert.
4. Speichern Sie die Änderungen.

Um die direkte Zuweisung eines Parameters zu entfernen

1. Wählen Sie den Tabreiter **Parameter**.
2. Wählen Sie in der Tabelle den Parameter, den Sie entfernen möchten.
3. Wenn der Parameter ausschließlich direkt zugewiesen ist, klicken Sie **Entfernen**.

   - ODER -

   Wenn der Parameter direkt und indirekt zugewiesen ist, deaktivieren Sie **Direkte Zuweisung**.
4. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Parameter auf Seite 95
- SAP Parameter an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 96
- SAP Parameter an Geschäftsrollen zuweisen auf Seite 98
- Vererbung von Parameterwerten an SAP Benutzerkonten auf Seite 100

Zusätzliche Aufgaben zur Verwaltung von SAP Benutzerkonten

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Überblick über das SAP Benutzerkonto

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das SAP Benutzerkonto**.

Ändern des Automatisierungsgrades an einem SAP Benutzerkonto

Wenn Sie Benutzerkonten über die automatische Personenzuordnung erstellen, wird der Standardautomatisierungsgrad genutzt. Sie können den Automatisierungsgrad eines Benutzerkontos nachträglich ändern.

Um den Automatisierungsgrad für ein Benutzerkonto zu ändern

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie auf dem Tabreiter **Adresse** in der Auswahlliste **Automatisierungsgrad** den Automatisierungsgrad.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten eines SAP Benutzerkontos auf Seite 136

SAP Gruppen und SAP Profile direkt an ein SAP Benutzerkonto zuweisen

Gruppen und Profile können einem Benutzerkonto direkt oder indirekt zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der Gruppen und Profile in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person ein SAP Benutzerkonto, werden die Gruppen und Profile der hierarchischen Rollen an dieses Benutzerkonto vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Gruppen und Profile direkt zuweisen.

HINWEIS:

- Es können nur solche Profile an Benutzerkonten zugewiesen werden, die keiner SAP Rolle zugeordnet sind.
- Es können keine generierten Profile an Benutzerkonten zugewiesen werden.
- Wenn das Benutzerkonto über eine ZBV administriert wird, können Gruppen und Profile aus allen Mandanten ausgewählt werden, denen das Benutzerkonto zugewiesen ist.

Um Gruppen oder Profile direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie eine der folgenden Aufgaben.
   - **Gruppen zuweisen**, um SAP Gruppen direkt zuzuweisen.
   - **Profile zuweisen**, um SAP Profile direkt zuzuweisen.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen oder Profile zu.

   - ODER -

Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen oder Profile.

5. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Gruppen, SAP Rollen und SAP Profile an SAP Benutzerkonten zuweisen auf Seite 173

SAP Rollen direkt an ein SAP Benutzerkonto zuweisen

Rollen können einem Benutzerkonto direkt oder indirekt zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der Rollen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person ein SAP Benutzerkonto, werden die SAP Rollen der hierarchischen Rollen an dieses Benutzerkonto vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Rollen direkt zuweisen.

Wenn das Benutzerkonto über eine ZBV administriert wird, können Rollen aus allen Mandanten ausgewählt werden, denen das Benutzerkonto zugewiesen ist.

Um Rollen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Rollen zuweisen**.

Um eine Rolle zuzuweisen

1. Klicken Sie **Hinzufügen**.

   Es wird eine neue Zeile in die Tabelle eingefügt.
2. Wählen Sie aus der Auswahlliste **Rolle**, die zuzuweisende Rolle aus.
3. Erfassen Sie bei Bedarf den Gültigkeitszeitraum der Rollenzuordnung in den Eingabefelder **Gültig von** und **Gültig bis**.
4. Weisen Sie bei Bedarf weitere Rollen zu.
5. Speichern Sie die Änderungen.

Um eine Rollenzuordnung zu bearbeiten

1. Wählen Sie in der Tabelle die Rollenzuordnung, die Sie bearbeiten möchten. Bearbeiten Sie den Gültigkeitszeitraum.
2. Speichern Sie die Änderungen.

Um eine Rollenzuordnung zu entfernen

1. Wählen Sie in der Tabelle die Rollenzuordnung, die Sie entfernen möchten.
2. Klicken Sie **Entfernen**.
3. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Benutzerkonten direkt an SAP Rollen zuweisen auf Seite 179
- Gültigkeitszeitraum von Rollenzuweisungen auf Seite 192

Strukturelle Profile zuweisen

Installierte Module: Modul SAP R/3 Strukturelle Profile Add-on

Strukturelle Profile können einem Benutzerkonto direkt oder indirekt zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der strukturellen Profile in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person ein SAP Benutzerkonto, werden die strukturellen Profile der hierarchischen Rollen an dieses Benutzerkonto vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die strukturellen Profile direkt zuweisen.

Um strukturelle Profile direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Strukturelle Profile zuweisen**.

Um ein strukturelles Profil zuzuweisen

1. Klicken Sie **Hinzufügen**.

   Es wird eine neue Zeile in die Tabelle eingefügt.
2. Wählen Sie aus der Auswahlliste **Strukturelles Profil**, das zuzuweisende strukturelle Profil aus.
3. Erfassen Sie bei Bedarf den Gültigkeitszeitraum der Profilzuordnung in den Eingabefelder **Gültig von** und **Gültig bis**.
4. Weisen Sie bei Bedarf weitere strukturelle Profile zu.
5. Speichern Sie die Änderungen.

Um eine Profilzuordnung zu bearbeiten

1. Wählen Sie in der Tabelle die Profilzuordnung, die Sie bearbeiten möchten. Bearbeiten Sie den Gültigkeitszeitraum.
2. Speichern Sie die Änderungen.

Um eine Profilzuordnung zu entfernen

1. Wählen Sie in der Tabelle die Profilzuordnung, die Sie entfernen möchten.
2. Klicken Sie **Entfernen**.
3. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- One Identity Manager Administrationshandbuch für das SAP R/3 Strukturelle Profile Add-on

Zugriff auf Mandaten einer Zentralen Benutzerverwaltung gewähren

Benutzerkonten, die über die Zentrale Benutzerverwaltung (ZBV) administriert werden, können über Zugriffsberechtigungen in verschiedenen Mandanten verfügen. Für jedes Benutzerkonto legen Sie fest, in welchen Mandanten es Zugriffsberechtigungen erhalten darf. Mandanten können indirekt und direkt zugewiesen werden. Für die indirekte Zuweisung erstellen Sie für die Mandanten Kontendefinitionen und weisen diese an hierarchische Rollen zu. Weitere Informationen finden Sie unter Zentrale Benutzerverwaltung im One Identity Manager auf Seite 133.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Mandanten direkt zuweisen. Dabei können das Zentralsystem und die Tochtersysteme ausgewählt werden. Einem Benutzerkonto können nur SAP Gruppen, Rollen oder Profile aus diesen Mandanten zugewiesen werden.

Die Aufgabe ist nur verfügbar, wenn der Mandant des ausgewählten Benutzerkontos als Zentralsystem gekennzeichnet ist.

Um ein Benutzerkonto direkt an einen Mandanten zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Mandanten einer ZBV zuweisen**.

Um einen Mandanten zuzuweisen

1. Klicken Sie **Hinzufügen**.

   Es wird eine neue Zeile in die Tabelle eingefügt.

2. Wählen Sie aus der Auswahlliste **Mandant** den Mandanten, in dem das Benutzerkonto Zugriffsberechtigungen erhalten soll.
3. Weisen Sie bei Bedarf eine Kontendefinition zu.
4. Weisen Sie bei Bedarf weitere Mandanten zu.
5. Speichern Sie die Änderungen.

Um eine Zuweisung zu bearbeiten

1. Wählen Sie in der Tabelle die Zuweisung, die Sie bearbeiten möchten. Bearbeiten Sie die Zuweisung der Kontendefinition.
2. Speichern Sie die Änderungen.

Um eine Zuweisung zu entfernen

1. Wählen Sie in der Tabelle die Zuweisung, die Sie entfernen möchten.
2. Klicken Sie **Entfernen**.
3. Speichern Sie die Änderungen.

SAP Lizenzen zuordnen

HINWEIS: Diese Aufgabe ist nur für Benutzerkonten verfügbar, die über eine ZBV verwaltet werden.

Für die Systemvermessung können den Benutzerkonten SAP Lizenzen in den Tochtersystemen und im Zentralsystem zugeordnet werden. Weitere Informationen finden Sie unter Bereitstellen der Daten für die Systemvermessung auf Seite 210.

Um einem Benutzerkonto Lizenzen zuzuordnen

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **SAP Lizenzen in Tochtersystem zuweisen**.
4. Klicken Sie **Hinzufügen**.

   Es wird eine neue Zeile in die Tabelle eingefügt.
5. Markieren Sie diese Zeile. Erfassen Sie die Vermessungsdaten.
6. Speichern Sie die Änderungen.

Um eine Lizenzzuordnung zu bearbeiten

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **SAP Lizenzen in Tochtersystem zuweisen**.
4. Wählen Sie in der Tabelle eine Zuordnung.

5. Bearbeiten Sie die Vermessungsdaten.
6. Speichern Sie die Änderungen.

Um eine Lizenzzuordnung zu entfernen

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **SAP Lizenzen in Tochtersystem zuweisen**.
4. Wählen Sie in der Tabelle eine Zuordnung.
5. Klicken Sie **Entfernen**.
6. Speichern Sie die Änderungen.

Auf dem Formular werden die folgenden Lizenzinformationen dargestellt.

Tabelle 53: Vermessungsdaten eines zentral verwalteten Benutzerkontos

Eigenschaft	Beschreibung
Empfängermandant	Mandant, in welchem dem Benutzerkonto eine Lizenz zugeordnet ist. Es kann das Zentralsystem oder ein zugeordnetes Tochtersystem ausgewählt werden.
Lizenz	Lizenz des Benutzerkontos im gewählten Mandanten.
Lizenzerweiterung	Lizenzerweiterung für die installierte Sonderversion. Wählen Sie aus der Auswahlliste die ID der Sonderversion.
Landeszuschlag	Zusätzliche Lizenzgebühr.
Abzurechnendes System	SAP System, in dem sich der abzurechnende Mandant befindet. Das Eingabefeld wird nur angezeigt, wenn als Lizenz "04 (Stellvertreter)" oder "11 (Multimandant/-system)" eingetragen ist.
Abzurechnender Mandant	Mandant, in dem sich das abzurechnende Benutzerkonto befindet. Das Eingabefeld wird nur angezeigt, wenn als Lizenz "04 (Stellvertreter)" oder "11 (Multimandant/-system)" eingetragen ist.
Abzurechnendes Benutzerkonto	Kostenpflichtiges Benutzerkonto, wenn als Lizenz "04 (Stellvertreter)" oder "11 (Multimandant/-system)" eingetragen ist.
Stellvertretend von	Zeitraum, in dem ein anderes Benutzerkonto die Stellvertretung übernimmt. Die Eingabefelder sind aktiviert, wenn als Lizenz "04 (Stellvertreter)" eingetragen ist.
Stellvertretend bis	

Verwandte Themen

- Sonderversionen auf Seite 105

SAP Benutzerkonto sperren und entsperren

Wie Sie Benutzerkonten sperren, ist abhängig von der Art der Verwaltung der Benutzerkonten. Benutzerkonten, die nicht mit einer Person verbunden sind, können über die Aufgabe **Benutzerkonto sperren** gesperrt werden.

Um ein Benutzerkonto zu sperren

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Benutzerkonto sperren**.
4. Schließen Sie die Meldung mit **OK**.

   Es wird ein Prozess generiert, der diese Änderung in das Zielsystem publiziert. Die Option **Benutzerkonto gesperrt** wird aktiviert, sobald der Prozess erfolgreich beendet wurde.

Ist das Benutzerkonto mit einer Person verbunden, wird das Benutzerkonto entsperrt, wenn ein neues zentrales Kennwort für die Person gesetzt wird. Das Verhalten wird über den Konfigurationsparameter **TargetSystem | SAPR3 | Accounts | UnlockByCentralPassword** gesteuert. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Um ein Benutzerkonto manuell zu entsperren

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das SAP Benutzerkonto.
3. Wählen Sie die Aufgabe **Benutzerkonto entsperren**.
4. Schließen Sie die Meldung mit **OK**.

   Es wird ein Prozess generiert, der diese Änderung in das Zielsystem publiziert. Die Option **Benutzerkonto gesperrt** wird deaktiviert, sobald der Prozess erfolgreich beendet wurde.

Detaillierte Informationen zum Thema

- Sperren von SAP Benutzerkonten auf Seite 162

Zusatzeigenschaften zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Zusatzeigenschaften.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

SAP Benutzerkonten umbenennen

Benutzerkonten können umbenannt werden, indem sie gelöscht und unter einem neuen Namen neu erstellt werden. Dabei werden bestehende Zuweisungen an das neue Benutzerkonto übernommen.

HINWEIS: Benutzerkonten mit dem Automatisierungsgrad **Full managed** können nicht umbenannt werden.

Um ein Benutzerkonto umzubenennen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **SAP Benutzerkonto umbenennen**.
5. Erfassen Sie den neuen Namen des Benutzerkontos und geben Sie das initiale Kennwort an.
6. Klicken Sie **OK**.

   Es werden Prozesse generiert, die diese Änderung in das Zielsystem publizieren.

Verwandte Themen

- Initiales Kennwort für neue SAP Benutzerkonten auf Seite 116

Automatische Zuordnung von Personen zu SAP Benutzerkonten

Tabelle 54: Konfigurationsparameter für die automatische Personenzuordnung

Konfigurationsparameter	Bedeutung
TargetSystem\SAPR3\PersonAutoFullsync	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem\SAPR3\PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem\SAPR3\PersonExcludeList	Der Konfigurationsparameter enthält eine Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird. Beispiel: `SAP*|SAPCPIC|SAPJSF|DDIC|J2EE_ADMIN|J2EE_GUEST`
TargetSystem\SAPR3\PersonAutoDisabledAccounts	Der Konfigurationsparameter legt fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.

Beim Einfügen eines Benutzerkontos kann automatisch eine vorhandene Person zugeordnet und im Bedarfsfall neu erstellt werden. Dabei werden die Personenstammdaten anhand vorhandener Benutzerstammdaten erzeugt. Dieser Mechanismus kann auf die Erstellung eines neuen Benutzerkontos durch manuelle Anlage oder Synchronisation folgen. Für die automatische Personenzuordnung definieren Sie Kriterien für die Ermittlung der Personen. Wird durch den eingesetzten Modus ein Benutzerkonto mit einer Person verbunden, so erhält das Benutzerkonto durch interne Verarbeitung den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Abhängig

davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden.

Schalten Sie das Verfahren im laufenden Betrieb ein, erfolgt ab diesem Zeitpunkt die automatische Zuordnung der Personen zu Benutzerkonten. Deaktivieren Sie das Verfahren zu einem späteren Zeitpunkt wieder, wirkt sich diese Änderung nur auf Benutzerkonten aus, die ab diesem Zeitpunkt angelegt oder aktualisiert werden. Bereits vorhandene Zuordnungen von Personen zu Benutzerkonten bleiben bestehen.

HINWEIS: Für administrative Benutzerkonten wird empfohlen, die Zuordnung der Personen nicht über die automatische Personenzuordnung vorzunehmen. Ordnen Sie Personen zu administrativen Benutzerkonten über die Aufgabe **Stammdaten bearbeiten** am jeweiligen Benutzerkonto zu.

Führen Sie folgende Aktionen aus, damit Personen automatisch zugeordnet werden können.

- Wenn Personen bei der Synchronisation von Benutzerkonten zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter „TargetSystem\SAPR3\PersonAutoFullsync“ und wählen Sie den gewünschte Modus.
- Wenn Personen außerhalb der Synchronisation zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter „TargetSystem\SAPR3\PersonAutoDefault“ und wählen Sie den gewünschten Modus.
- Legen Sie im Konfigurationsparameter "TargetSystem\SAPR3\PersonExcludeList" die Benutzerkonten fest, für die keine automatische Zuordnung zu Personen erfolgen soll.

  Beispiel:

  `SAP*|SAPCPIC|SAPJSF|DDIC|J2EE_ADMIN|J2EE_GUEST`
- Legen Sie über den Konfigurationsparameter "TargetSystem\SAPR3\PersonAutoDisabledAccounts" fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
- Weisen Sie dem Mandanten eine Kontendefinition zu. Stellen Sie sicher, dass der Automatisierungsgrad, der verwendet werden soll, als Standardautomatisierungsgrad eingetragen ist.
- Definieren Sie die Suchkriterien für die Personenzuordnung am Mandanten.

HINWEIS:

Für die Synchronisation gilt:

- Die automatische Personenzuordnung wirkt, wenn Benutzerkonten neu angelegt oder aktualisiert werden.

Außerhalb der Synchronisation gilt:

- Die automatische Personenzuordnung wirkt, wenn Benutzerkonten neu angelegt werden.

HINWEIS:

Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Personen erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für den Mandanten bekannt, werden die Benutzerkonten mit den Personen verbunden. Es wird jedoch noch keine Kontendefinition zugewiesen. Die Benutzerkonten sind somit im Zustand **Linked** (verbunden).

Um die Benutzerkonten über Kontendefinitionen zu verwalten, weisen Sie diesen Benutzerkonten eine Kontendefinition und einen Automatisierungsgrad zu.

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie dem Mandanten die Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand **Linked** (verbunden) die Kontendefinition zu. Es wird der Standardautomatisierungsgrad der Kontendefinition für das Benutzerkonto übernommen.
    a. Wählen Sie im Manager die Kategorie **SAP R/3 | Benutzerkonten | Verbunden aber nicht konfiguriert | <Mandant>**.
    b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.
    c. Wählen Sie in der Auswahlliste **Kontendefinition** die Kontendefinition.
    d. Wählen Sie die Benutzerkonten, die die Kontendefinition erhalten sollen.
    e. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul

Verwandte Themen

- Erstellen einer Kontendefinition auf Seite 67
- Zuweisen der Kontendefinition an ein Zielsystem auf Seite 82
- Bearbeiten der Suchkriterien für die automatische Personenzuordnung auf Seite 158

Bearbeiten der Suchkriterien für die automatische Personenzuordnung

Die Kriterien für die Personenzuordnung werden am Mandanten definiert. Dabei legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person dem Benutzerkonto zugeordnet werden kann. Die Suchkriterien können Sie durch Formatdefinitionen weiter einschränken. Das zusammengestellte Suchkriterium wird in XML-Notation in die Spalte **Suchkriterien für die automatische Personenzuordnung** (`AccountToPersonMatchingRule`) der Tabelle `SAPMandant` geschrieben.

Suchkriterien werden bei der automatischen Zuordnung von Personen zu Benutzerkonten ausgewertet. Darüber hinaus können Sie anhand der Suchkriterien eine Vorschlagsliste für die Personenzuordnung an Benutzerkonten erzeugen und die Zuordnung direkt ausführen.

HINWEIS: Bei der Zuordnung der Personen zu Benutzerkonten anhand der Suchkriterien erhalten die Benutzerkonten den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Abhängig davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden.

Für administrative Benutzerkonten wird empfohlen, die Zuordnung nicht anhand der Suchkriterien vorzunehmen. Ordnen Sie Personen zu administrativen Benutzerkonten über die Aufgabe **Stammdaten bearbeiten** am jeweiligen Benutzerkonto zu.

HINWEIS: Der One Identity Manager liefert ein Standardmapping für die Personenzuordnung. Führen Sie die folgenden Schritte nur aus, wenn Sie das Standardmapping unternehmensspezifisch anpassen möchten.

Um Kriterien für die Personenzuordnung festzulegen

1. Wählen Sie die Kategorie **SAP R/3 | Mandanten**.
2. Wählen Sie in der Ergebnisliste den Mandanten.
3. Wählen Sie die Aufgabe **Suchkriterien für die Personenzuordnung definieren**.
4. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person mit dem Benutzerkonto verbunden wird.

   Tabelle 55: Standardsuchkriterien für Benutzerkonten

Anwenden auf	Spalte an Person	Spalte am Benutzerkonto
SAP Benutzerkonten des Typs "Dialog"	Zentrales SAP Benutzerkonto (`CentralSAPAccount`)	Benutzerkonto (`Accnt`)

5. Speichern Sie die Änderungen.

Direkte Zuordnung von Personen an Benutzerkonten anhand einer Vorschlagsliste

Im Bereich **Zuordnungen** können Sie anhand der Suchkriterien eine Vorschlagsliste für die Personenzuordnung an Benutzerkonten erzeugen und die Zuordnung direkt ausführen. Die Benutzerkonten sind dafür in verschiedenen Ansichten zusammengestellt.

Tabelle 56: Ansichten zur manuellen Zuordnung

Ansicht	Beschreibung
Vorgeschlagene Zuordnungen	Die Ansicht listet alle Benutzerkonten auf, denen der One Identity Manager eine Person zuordnen kann. Dazu werden die Personen

Ansicht	Beschreibung
	angezeigt, die durch die Suchkriterien ermittelt und zugeordnet werden können.
Zugeordnete Benutzerkonten	Die Ansicht listet alle Benutzerkonten auf, denen eine Person zugeordnet ist.
Ohne Personenzuordnung	Die Ansicht listet alle Benutzerkonten auf, denen keine Person zugeordnet ist und für die über die Suchkriterien keine passende Person ermittelt werden kann.

TIPP: Mit Maus-Doppelklick auf einen Eintrag in den Ansichten werden das Benutzerkonto und die Person geöffnet und Sie können die Stammdaten einsehen.

Um die Suchkriterien auf die Benutzerkonten anzuwenden

- Klicken Sie **Neu laden**.

  Für alle Benutzerkonten im Zielsystem werden die möglichen Zuordnungen anhand der Suchkriterien ermittelt. Die drei Ansichten werden aktualisiert.

Um Personen direkt über die Vorschlagsliste zuzuordnen

1. Klicken Sie **Vorgeschlagene Zuordnungen**.
   a. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die vorgeschlagene Person zugeordnet werden soll. Eine Mehrfachauswahl ist möglich.
   b. Klicken Sie **Ausgewählte zuweisen.**
   c. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

      Den ausgewählten Benutzerkonten werden die per Suchkriterium ermittelten Personen zugeordnet.

   – ODER –
2. Klicken Sie **Ohne Personenzuordnung**.
   a. Klicken Sie **Person auswählen** für das Benutzerkonto, dem eine Person zugeordnet werden soll. Wählen Sie eine Person aus der Auswahlliste.
   b. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die ausgewählten Personen zugeordnet werden sollen. Eine Mehrfachauswahl ist möglich.
   c. Klicken Sie **Ausgewählte zuweisen**.
   d. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

      Den ausgewählten Benutzerkonten werden die Personen zugeordnet, die in der Spalte **Person** angezeigt werden.

Um Zuordnungen zu entfernen

1. Klicken Sie **Zugeordnete Benutzerkonten**.
   a. Klicken Sie **Auswahl** für alle Benutzerkonten, deren Personenzuordnung entfernt werden soll. Mehrfachauswahl ist möglich.

b. Klicken Sie **Ausgewählte entfernen**.

c. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Von den ausgewählten Benutzerkonten werden die zugeordneten Personen entfernt.

Ausführliche Informationen zur Definition der Suchkriterien finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Automatische Zuordnung von Personen zu SAP Benutzerkonten auf Seite 156

Automatisches Erzeugen von Abteilungen anhand von SAP Benutzerkonteninformationen

Anhand der Abteilungsinformationen der Benutzerkonten können neue Abteilungen im One Identity Manager erzeugt werden. Zusätzlich werden die Abteilungen den Personen der Benutzerkonten als primäre Abteilung zugeordnet. Bei entsprechender Konfiguration des One Identity Manager können die Personen über diese Zuordnungen ihre Unternehmensressourcen erhalten.

Voraussetzungen für den Einsatz dieses Verfahrens

- Personen müssen beim Anlegen und Ändern von Benutzerkonten automatisch erzeugt werden. Mindestens einer der folgenden Konfigurationsparameter muss aktiviert sein und das entsprechende Verfahren eingerichtet sein.

  Tabelle 57: Konfigurationsparameter für automatische Personenzuordnung

Konfigurationsparameter	Wirkung bei Aktivierung
TargetSystem | SAPR3 | PersonAutoDefault	Anhand des angegebenen Modus werden Personen automatisch an Benutzerkonten zugeordnet, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem | SAPR3 | PersonAutoFullsync	Anhand des angegebenen Modus werden Personen automatisch an Benutzerkonten zugeordnet, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.

- Es ist kein Synchronisationsprojekt für Personalplanungsdaten eingerichtet.

Bei der Synchronisation von Personalplanungsdaten werden Abteilungen, die bereits aus SAP Benutzerkonteninformationen erzeugt wurden, als ausstehend markiert. Nutzen Sie das Verfahren zum automatischen Erzeugen von Abteilungen aus Benutzerkonteninformationen nur dann, wenn Abteilungen nicht durch die Synchronisation von Personalplanungsdaten in der Datenbank angelegt werden. Ausführliche Informationen zur Synchronisation von Personalplanungsdaten finden Sie im *One Identity Manager Administrationshandbuch für das SAP R/3 Strukturelle Profile Add-on*.

Um Abteilungen aus den Benutzerkonteninformationen zu erzeugen

- Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | SAPR3 | AutoCreateDepartment**.

  Für alle Abteilungen, die auf diesem Weg in der One Identity Manager-Datenbank erzeugt wurden, ist als Datenquelle Import **SAP R/3** angegeben (Spalte `ImportSource='SAP'`).

Verwandte Themen

- Allgemeine Stammdaten eines SAP Benutzerkontos auf Seite 136
- Automatische Zuordnung von Personen zu SAP Benutzerkonten auf Seite 156

Sperren von SAP Benutzerkonten

Wie Sie Benutzerkonten sperren, ist abhängig von der Art der Verwaltung der Benutzerkonten.

Szenario:

- Die Benutzerkonten sind mit Personen verbunden und werden über Kontendefinitionen verwaltet.

Benutzerkonten, die über Kontendefinitionen verwaltet werden, werden gesperrt, wenn die Person dauerhaft oder zeitweilig deaktiviert wird. Das Verhalten ist abhängig vom Automatisierungsgrad des Benutzerkontos. Benutzerkonten mit dem Automatisierungsgrad **Full managed** werden entsprechend der Einstellungen an der Kontendefinition deaktiviert. Auf diese Benutzerkonten können die Aufgaben **Benutzerkonto sperren** und **Benutzerkonto entsperren** nicht angewendet werden. Für Benutzerkonten mit einem anderen Automatisierungsgrad konfigurieren Sie das gewünschte Verhalten an der Bildungsregel der Spalte `SAPUser.U_Flag`.

Szenario:

- Die Benutzerkonten sind mit Personen verbunden. Es sind keine Kontendefinitionen zugeordnet.

Benutzerkonten, die mit Personen verbunden sind, jedoch nicht über Kontendefinitionen verwaltet werden, werden gesperrt, wenn die Person dauerhaft oder zeitweilig deaktiviert wird. Das Verhalten ist abhängig vom Konfigurationsparameter **QER | Person | TemporaryDeactivation**.

- Ist der Konfigurationsparameter aktiviert, werden die Benutzerkonten einer Person gesperrt, wenn die Person zeitweilig oder dauerhaft deaktiviert wird. Auf diese Benutzerkonten können die Aufgaben **Benutzerkonto sperren** und **Benutzerkonto entsperren** nicht angewendet werden.
- Ist der Konfigurationsparameter deaktiviert, haben die Eigenschaften der Person keinen Einfluss auf die verbundenen Benutzerkonten.

Um das Benutzerkonto bei deaktiviertem Konfigurationsparameter zu sperren

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Benutzerkonto sperren**.
4. Schließen Sie die Meldung mit **OK**.

Szenario:

- Benutzerkonten sind nicht mit Personen verbunden.

Um ein Benutzerkonto zu sperren, das nicht mit einer Person verbunden ist

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Benutzerkonto sperren**.
4. Schließen Sie die Meldung mit **OK**.

Es wird ein Prozess generiert, der diese Änderung am Benutzerkonto in das Zielsystem publiziert. Sobald die Sperrung in das Zielsystem publiziert wurde, ist die Option **Benutzerkonto gesperrt** auf dem Stammdatenformular, Tabreiter **Logondaten** aktiviert. Der Benutzer kann sich nicht mehr mit diesem Benutzerkonto am Zielsystem anmelden.

Um ein Benutzerkonto zu entsperren

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Benutzerkonto entsperren**.
4. Schließen Sie die Meldung mit **OK**.

   Es wird ein Prozess generiert, der diese Änderung in das Zielsystem publiziert. Die Option **Benutzerkonto gesperrt** wird deaktiviert, sobald der Prozess erfolgreich beendet wurde.

Detaillierte Informationen zum Thema

Weitere Informationen finden Sie imOne Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

Verwandte Themen

- Einrichten von Kontendefinitionen auf Seite 66
- Erstellen der Automatisierungsgrade auf Seite 69

Löschen und Wiederherstellen von SAP Benutzerkonten

HINWEIS: Solange eine Kontendefinition für eine Person wirksam ist, behält die Person ihr daraus entstandenes Benutzerkonto. Wird die Zuweisung einer Kontendefinition entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht.

Um ein Benutzerkonto zu löschen

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie , um das Benutzerkonto zu löschen.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Um ein Benutzerkonto wiederherzustellen

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste .

Konfigurieren der Löschverzögerung

Standardmäßig werden Benutzerkonten mit einer Löschverzögerung von 30 Tagen endgültig aus der Datenbank entfernt. Die Benutzerkonten werden zunächst deaktiviert. Bis zum Ablauf der Löschverzögerung besteht die Möglichkeit die Benutzerkonten wieder zu aktivieren. Nach Ablauf der Löschverzögerung werden die Benutzerkonten aus der Datenbank gelöscht und ein Wiederherstellen ist nicht mehr möglich. Eine abweichende Löschverzögerung konfigurieren Sie im Designer an der Tabelle SAPUser. Die Löschverzögerung hat keinen Einfluss auf die Anmeldeerlaubnis in den zugeordneten Tochtermandanten einer ZBV.

Erfassen von externen Benutzerkennungen für ein SAP Benutzerkonto

In einer SAP R/3-Umgebung können externe Authentifizierungsmechanismen zu Anmeldung an einem System genutzt werden. Der One Identity Manager ermöglicht die Pflege der Anmeldedaten für die Anmeldung von Benutzern externer Systeme, wie beispielsweise Active Directory, an einer SAP R/3-Umgebung.

Mit dem One Identity Manager können externe Benutzerkennungen erfasst und gelöscht werden. Für bestehende Benutzerkennungen kann nur die Option "Konto ist aktiviert" bearbeitet werden.

Um externe Kennungen zu erfassen

1. Wählen Sie die Kategorie **SAP R/3 | Externe Kennungen**.
2. Wählen Sie in der Ergebnisliste die externe Kennung. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Für eine externe Benutzerkennung erfassen Sie folgende Daten.

Tabelle 58: Eigenschaften einer externen Kennung

Eigenschaft	Beschreibung
Externe Benutzerkennung	Anmeldename, mit dem sich der Benutzer am externen System anmeldet. Die Syntax ist abhängig von der gewählten Authentifizierungsart. Die vollständige Benutzerkennung wird per Bildungsregel zusammengesetzt. HINWEIS: Das BAPI des One Identity Manager nutzt für die Generierung der Benutzerkennung die Standardeinstellungen des Programmes RSUSREXT, das heißt der Benutzername wird der externen Kennung nachgestellt. Der in der Schnittstelle bereitgestellte Wert wird als Präfix übergeben. Wenn Ihre SAP R/3-Umgebung andere als diese Standardeinstellungen nutzt, passen Sie die Bildungsregel für die Spalte SAPUserExtId.EXTID entsprechend an.
Typ der externen Kennung	Authentifizierungsart für den externen Benutzer. Daraus ergibt sich die Syntax für die externe Kennung.

Eigenschaft	Beschreibung
	Tabelle 59: Typen für externe Kennungen Definierter Name für X.509 — Die Anmeldung erfolgt über den Distinguished Name für X.509. Windows NTLM oder Kennwortverifizierung — Die Anmeldung erfolgt über Windows NT Lan Manager oder Kennwortverifizierung mit dem Windows-Domänen-Controller. LDAP-Bind <benutzerdefiniert> — Die Anmeldung erfolgt über LDAP Bind (für andere externe Authentifizierungsmechanismen). SAML Token — Die Authentifizierung erfolgt über ein SAML-Token-Profil. Der Standardtyp ist im Konfigurationsparameter "TargetSystem\SAPR3\Accounts\ExtID_Type" festgelegt.
Zielsystemtyp	Wird zusammen mit dem Typ der externen Kennung zur Überprüfung der Anmeldedaten herangezogen. Der Standardwert ist im Konfigurationsparameter "TargetSystem\SAPR3\Accounts\TargetSystemID" festgelegt. Zulässige Werte sind `ADSACCOUNT` und `NTACCOUNT`.
Konto ist aktiviert	Angabe, ob sich der Benutzer über ein externes Authentifizierungssystem am System anmelden kann.
Benutzerkonto	Zuordnung der externen Kennung zu einem Benutzerkonto.
Laufende Nummer	Laufende Nummer, wenn ein Benutzerkonto mehrere externe Kennungen besitzt.
Gültig von	Datum, ab dem die externe Benutzerkennung gültig ist.

Verwandte Themen

- Typen für externe Kennungen auf Seite 94

8

SAP Gruppen, SAP Rollen und SAP Profile

Um den Benutzerkonten die benötigten Berechtigungen zur Verfügung zu stellen, werden im One Identity Manager Gruppen, Rollen und Profile abgebildet. Gruppen, Rollen und Profile können im One Identity Manager an Benutzerkonten zugewiesen, bestellt oder über hierarchische Rollen vererbt werden. Es können keine Gruppen, Rollen oder Profile neu angelegt oder gelöscht werden.

Gruppen

Mit der Zuordnung von Benutzerkonten zu Gruppen können Sie die Pflege der Benutzerkonten auf unterschiedliche Benutzeradministratoren verteilen.

Rollen

Eine Rolle umfasst alle Transaktionen und Benutzermenüs, die ein SAP Benutzer für seine Aufgaben benötigt. Rollen werden in Einzelrollen und Sammelrollen unterschieden. Einzelrollen können in Sammelrollen zusammengefasst werden. Die Mitgliedschaft eines Benutzerkontos in den Rollen kann zeitlich begrenzt sein.

Profile

Über Profile werden die Zugriffsrechte auf das System geregelt. Profile werden über Einzelrollen oder direkt an Benutzerkonten zugewiesen. Profile können zu Sammelprofilen zusammengefasst sein.

Bearbeiten der Stammdaten für SAP Gruppen, SAP Rollen und SAP Profile

Im One Identity Manager können Sie folgende Informationen über Gruppen, Rollen und Profile bearbeiten:

- Zugewiesene SAP Benutzerkonten
- Nutzung im IT Shop
- Risikobewertung
- Vererbung über hierarchische Rollen und Einschränkung der Vererbung
- Lizenzinformationen für die Systemvermessung

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie die Kategorie **SAP R/3 | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Um die Stammdaten eines Profils zu bearbeiten

1. Wählen Sie die Kategorie **SAP R/3 | Profile**.
2. Wählen Sie in der Ergebnisliste das Profil. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Um die Stammdaten einer Rolle zu bearbeiten

1. Wählen Sie die Kategorie **SAP R/3 | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten von SAP Gruppen auf Seite 169
- Allgemeine Stammdaten von SAP Rollen auf Seite 170
- Allgemeine Stammdaten von SAP Profilen auf Seite 171

Allgemeine Stammdaten von SAP Gruppen

Tabelle 60: Konfigurationsparameter für die Risikobewertung von SAP Benutzerkonten

Konfigurationsparameter	Wirkung bei Aktivierung
QER\CalculateRiskIndex	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Berechnung des Risikoindex. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Werte für den Risikoindex erfasst und berechnet werden.

Für eine Gruppe bearbeiten Sie folgende Stammdaten.

Tabelle 61: Stammdaten von SAP Gruppen

Eigenschaft	Beschreibung
Anzeigename	Name der Gruppe zur Anzeige in den One Identity Manager-Werkzeugen. Wird standardmäßig aus der Bezeichnung der Gruppe gebildet.
Bezeichnung	Bezeichnung der Gruppe im Zielsystem.
Mandant	Mandant, in dem die Gruppe angelegt ist.
Leistungsposition	Angabe einer Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist.
Kategorie	Kategorien für die Vererbung von Gruppen. Gruppen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Shop	Angabe, ob die Gruppe über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.

Detaillierte Informationen zum Thema

- Festlegen der Kategorien für die Vererbung von SAP Gruppen, SAP Rollen und SAP Profilen auf Seite 125
- One Identity Manager Administrationshandbuch für IT Shop
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul
- One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul
- One Identity Manager Administrationshandbuch für Risikobewertungen

Allgemeine Stammdaten von SAP Rollen

Tabelle 62: Konfigurationsparameter für die Risikobewertung von SAP Benutzerkonten

Konfigurationsparameter	Wirkung bei Aktivierung
QER\CalculateRiskIndex	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Berechnung des Risikoindex. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Werte für den Risikoindex erfasst und berechnet werden.

Für eine Rolle bearbeiten Sie folgende Stammdaten.

Tabelle 63: Stammdaten von SAP Rollen

Eigenschaft	Beschreibung
Anzeigename	Name der Rolle zur Anzeige in den One Identity Manager-Werkzeugen. Wird standardmäßig aus der Bezeichnung der Rolle gebildet.
Bezeichnung	Bezeichnung der Rolle im Zielsystem.
Mandant	Mandant, in dem die Rolle angelegt ist.
Lizenz	Lizenz der Rolle. Diese Angabe wird für die Ermittlung der Systemvermessungsdaten für Benutzerkonten benötigt und ist nach der Synchronisation einmalig zuzuordnen.
Rollentyp	Rollentyp zur Unterscheidung von Einzelrollen und Sammelrollen.
Leistungsposition	Angabe einer Leistungsposition, um die Rolle über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Rolle an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das

Eigenschaft	Beschreibung
	Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter „QER\CalculateRiskIndex“ aktiviert ist.
Kategorie	Kategorien für die Vererbung von Rollen. Rollen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Rollen und die Benutzerkonten in Kategorien eingeteilt. Über die Auswahlliste ordnen Sie die Rolle einer oder mehreren Kategorien zu.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Rollenbeschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Shop	Angabe, ob die Rolle über den IT Shop bestellbar ist. Die Rolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Rolle kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Rolle ausschließlich über den IT Shop bestellbar ist. Die Rolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Rolle an hierarchische Rollen ist nicht zulässig.

Detaillierte Informationen zum Thema

- Lizenzen auf Seite 104
- Bereitstellen der Daten für die Systemvermessung auf Seite 210
- Festlegen der Kategorien für die Vererbung von SAP Gruppen, SAP Rollen und SAP Profilen auf Seite 125
- One Identity Manager Administrationshandbuch für IT Shop
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul
- One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul
- One Identity Manager Administrationshandbuch für Risikobewertungen

Allgemeine Stammdaten von SAP Profilen

Tabelle 64: Konfigurationsparameter für die Risikobewertung von SAP Benutzerkonten

Konfigurationsparameter	Wirkung bei Aktivierung
QER\CalculateRiskIndex	Präprozessorrelevanter Konfigurationsparameter zur

Konfigurationsparameter	Wirkung bei Aktivierung
	Steuerung der Modellbestandteile für die Berechnung des Risikoindex. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Werte für den Risikoindex erfasst und berechnet werden.

Für ein Profil bearbeiten Sie folgende Stammdaten.

Tabelle 65: Stammdaten von SAP Profilen

Eigenschaft	Beschreibung
Anzeigename	Name des Profils zur Anzeige in den One Identity Manager-Werkzeugen. Wird standardmäßig aus der Bezeichnung des Profils gebildet.
Bezeichnung	Bezeichnung des Profils im Zielsystem.
Mandant	Mandant, in dem das Profil angelegt ist.
Lizenz	Lizenz des Profils. Diese Angabe wird für die Ermittlung der Systemvermessungsdaten für SAP Benutzerkonten benötigt und ist nach der Synchronisation einmalig zuzuordnen.
Profiltyp	Profiltyp zur Unterscheidung von Einzelprofilen, Sammelprofilen und generierten Profilen.
Leistungsposition	Angabe einer Leistungsposition, um das Profil über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen des Profils an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter „QER\CalculateRiskIndex" aktiviert ist.
Kategorie	Kategorien für die Vererbung von Profilen. Profile können selektiv an Benutzerkonten vererbt werden. Dazu werden die Profile und die Benutzerkonten in Kategorien eingeteilt. Über die Auswahlliste ordnen Sie das Profil einer oder mehreren Kategorien zu.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Profil ist aktiv	Angabe, ob es sich um ein aktives Profil oder eine Pflegeversion des Profils handelt.
Zuweisung eingeschränkt	Angabe, ob das Profil einer SAP Rolle zugeordnet ist. Das Profil kann damit nicht direkt an Benutzerkonten, Geschäftsrollen, Organisationen oder IT Shop Regale zugewiesen werden.
IT Shop	Angabe, ob das Profil über den IT Shop bestellbar ist. Das Profil kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Das Profil kann

Eigenschaft	Beschreibung
	weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden. Für generierte Profile kann die Option nicht aktiviert werden.
Verwendung nur im IT Shop	Angabe, ob das Profil ausschließlich über den IT Shop bestellbar ist. Das Profil kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung des Profils an hierarchische Rollen ist nicht zulässig. Für generierte Profile kann die Option nicht aktiviert werden.

Detaillierte Informationen zum Thema

- Lizenzen auf Seite 104
- Bereitstellen der Daten für die Systemvermessung auf Seite 210
- Festlegen der Kategorien für die Vererbung von SAP Gruppen, SAP Rollen und SAP Profilen auf Seite 125
- One Identity Manager Administrationshandbuch für IT Shop
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul
- One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul
- One Identity Manager Administrationshandbuch für Risikobewertungen

SAP Gruppen, SAP Rollen und SAP Profile an SAP Benutzerkonten zuweisen

Gruppen, Rollen und Profile können direkt oder indirekt an Benutzerkonten zugewiesen werden. Bei der indirekten Zuweisung werden Personen, Gruppen, Rollen und Profile in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der Gruppen, Rollen und Profile, die einer Person zugewiesen ist. Wenn Sie eine Person in hierarchische Rollen aufnehmen und die Person ein Benutzerkonto besitzt, dann wird dieses Benutzerkonto in die Gruppe, die Rolle oder das Profile aufgenommen. Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind:

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und Gruppen, Rollen und Profilen erlaubt.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.
- Die Benutzerkonten, Gruppen, Rollen und Profile gehören zum selben SAP Mandanten.

Des Weiteren können Gruppen, Rollen und Profile über IT Shop-Bestellungen an Personen zugewiesen werden. Damit Gruppen, Rollen und Profile über IT Shop-Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle Gruppen, Rollen und Profile, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Gruppen, Rollen und Profile werden nach erfolgreicher Genehmigung den Personen zugewiesen.

HINWEIS: Es können nur solche Profile an hierarchische Rollen zugewiesen werden, die keiner SAP Rolle zugeordnet sind.

Detaillierte Informationen zum Thema

- SAP Gruppen, SAP Rollen und SAP Profile an Organisationen zuweisen auf Seite 174
- SAP Gruppen, SAP Rollen und SAP Profile an Geschäftsrollen zuweisen auf Seite 176
- SAP Benutzerkonten direkt an SAP Gruppen und SAP Profile zuweisen auf Seite 178
- SAP Gruppen, SAP Rollen und SAP Profile in Systemrollen aufnehmen auf Seite 180
- SAP Gruppen, SAP Rollen und SAP Profile in den IT Shop aufnehmen auf Seite 182
- Zuordnung und Vererbung von SAP Profilen und SAP Rollen an SAP Benutzerkonten auf Seite 184
- Gültigkeitszeitraum von Rollenzuweisungen auf Seite 192
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

SAP Gruppen, SAP Rollen und SAP Profile an Organisationen zuweisen

Weisen Sie Gruppen, Rollen und Profile an Abteilungen, Kostenstellen oder Standorte zu, damit sie über diese Organisationen an Benutzerkonten zugewiesen werden.

Um eine Gruppe an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **SAP R/3 | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Organisationen.

5. Speichern Sie die Änderungen.

Um eine Rolle an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **SAP R/3 | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
    - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
    - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
    - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

    - ODER -

    Entfernen Sie im Bereich **Zuordnungen entfernen** die Organisationen.
5. Speichern Sie die Änderungen.

Um ein Profil an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **SAP R/3 | Profile**.
2. Wählen Sie in der Ergebnisliste das Profil.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
    - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
    - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
    - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

    - ODER -

    Entfernen Sie im Bereich **Zuordnungen entfernen** die Organisationen.
5. Speichern Sie die Änderungen.

Um Gruppen, Rollen oder Profile an eine Abteilung, eine Kostenstellen oder einen Standorte zuzuweisen (bei rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **Organisationen | Abteilungen**.

    - ODER -

    Wählen Sie die Kategorie **Organisationen | Kostenstellen**.

    - ODER -

    Wählen Sie die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **SAP Gruppen zuweisen**.

    - ODER -

Wählen Sie die Aufgabe **SAP Rollen zuweisen**.

- ODER -

Wählen Sie die Aufgabe **SAP Profile zuweisen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen, Rollen oder Profile zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen, Rollen oder Profile.
5. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Gruppen, SAP Rollen und SAP Profile an Geschäftsrollen zuweisen auf Seite 176
- SAP Benutzerkonten direkt an SAP Gruppen und SAP Profile zuweisen auf Seite 178
- SAP Gruppen, SAP Rollen und SAP Profile in Systemrollen aufnehmen auf Seite 180
- SAP Gruppen, SAP Rollen und SAP Profile in den IT Shop aufnehmen auf Seite 182
- One Identity Manager Benutzer für die Verwaltung einer SAP R/3-Umgebung auf Seite 12

SAP Gruppen, SAP Rollen und SAP Profile an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie Gruppen, Rollen und Profile an Geschäftsrollen zu, damit sie über diese Geschäftsrollen an Benutzerkonten zugewiesen werden.

Um eine Gruppe an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **SAP R/3 | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
5. Speichern Sie die Änderungen.

Um eine Rolle an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **SAP R/3 | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
5. Speichern Sie die Änderungen.

Um ein Profil an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **SAP R/3 | Profile**.
2. Wählen Sie in der Ergebnisliste das Profil.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
5. Speichern Sie die Änderungen.

Um Gruppen, Rollen oder Profile an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **SAP Gruppen zuweisen**.

   - ODER -

   Wählen Sie die Aufgabe **SAP Rollen zuweisen**.

   - ODER -

   Wählen Sie die Aufgabe **SAP Profile zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen, Rollen oder Profile zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen, Rollen oder Profile.
5. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Gruppen, SAP Rollen und SAP Profile an Organisationen zuweisen auf Seite 174
- SAP Benutzerkonten direkt an SAP Gruppen und SAP Profile zuweisen auf Seite 178

- SAP Gruppen, SAP Rollen und SAP Profile in Systemrollen aufnehmen auf Seite 180
- SAP Gruppen, SAP Rollen und SAP Profile in den IT Shop aufnehmen auf Seite 182
- One Identity Manager Benutzer für die Verwaltung einer SAP R/3-Umgebung auf Seite 12

SAP Benutzerkonten direkt an SAP Gruppen und SAP Profile zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Gruppen und Profile direkt an Benutzerkonten zuweisen.

HINWEIS:

- Es können nur solche Profile an Benutzerkonten zugewiesen werden, die keiner SAP Rolle zugeordnet sind.
- Es können keine generierten Profile an Benutzerkonten zugewiesen werden.

Wenn die Benutzerkonten über eine ZBV administriert werden, gilt:

- Die Gruppe (das Profil) ist dem Zentralsystem zugeordnet, oder
- Der Mandant der Gruppe (des Profils) ist den Benutzerkonten als Tochtersystem zugewiesen.

Um eine Gruppe direkt an Benutzerkonten zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
5. Speichern Sie die Änderungen.

Um ein Profil direkt an Benutzerkonten zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Profile**.
2. Wählen Sie in der Ergebnisliste das Profil.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
5. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Gruppen und SAP Profile direkt an ein SAP Benutzerkonto zuweisen auf Seite 148
- SAP Gruppen, SAP Rollen und SAP Profile an Organisationen zuweisen auf Seite 174
- SAP Gruppen, SAP Rollen und SAP Profile an Geschäftsrollen zuweisen auf Seite 176
- SAP Gruppen, SAP Rollen und SAP Profile in Systemrollen aufnehmen auf Seite 180
- SAP Gruppen, SAP Rollen und SAP Profile in den IT Shop aufnehmen auf Seite 182

SAP Benutzerkonten direkt an SAP Rollen zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie Rollen direkt an Benutzerkonten zuweisen.

Wenn die Benutzerkonten über eine ZBV administriert werden, gilt:

- Die Rolle ist dem Zentralsystem zugeordnet, oder
- Der Mandant der Rolle ist den Benutzerkonten als Tochtersystem zugewiesen.

Um eine Rolle direkt an Benutzerkonten zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.

Um eine Rolle an ein Benutzerkonto zuzuweisen

1. Klicken Sie **Hinzufügen**.

   Es wird eine neue Zeile in die Tabelle eingefügt.
2. Wählen Sie aus der Auswahlliste **Benutzerkonto**, das Benutzerkonto aus, dem die Rolle zugewiesen werden soll.
3. Erfassen Sie bei Bedarf den Gültigkeitszeitraum der Rollenzuordnung in den Eingabefelder **Gültig von** und **Gültig bis**.
4. Fügen Sie bei Bedarf weitere Benutzerkonten hinzu.
5. Speichern Sie die Änderungen.

Um eine Rollenzuordnung zu bearbeiten

1. Wählen Sie in der Tabelle die Rollenzuordnung, die Sie bearbeiten möchten. Bearbeiten Sie den Gültigkeitszeitraum.
2. Speichern Sie die Änderungen.

Um eine Rollenzuordnung zu entfernen

1. Wählen Sie in der Tabelle die Rollenzuordnung, die Sie entfernen möchten.
2. Klicken Sie **Entfernen**.
3. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Rollen direkt an ein SAP Benutzerkonto zuweisen auf Seite 149
- SAP Gruppen, SAP Rollen und SAP Profile an Organisationen zuweisen auf Seite 174
- SAP Gruppen, SAP Rollen und SAP Profile an Geschäftsrollen zuweisen auf Seite 176
- SAP Gruppen, SAP Rollen und SAP Profile in Systemrollen aufnehmen auf Seite 180
- SAP Gruppen, SAP Rollen und SAP Profile in den IT Shop aufnehmen auf Seite 182

SAP Gruppen, SAP Rollen und SAP Profile in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

Gruppen, Rollen und Profile können in verschiedene Systemrollen aufgenommen werden. Wenn Sie eine Systemrolle an Personen zuweisen, werden die Gruppen, Rollen und Profile an alle SAP Benutzerkonten vererbt, die diese Personen besitzen. Systemrollen, in der ausschließlich SAP Gruppen, Rollen oder Profile zusammengefasst sind, können mit dem Systemrollentyp „SAP Produkt" gekennzeichnet werden. Gruppen, Rollen und Profile können auch in Systemrollen aufgenommen werden, die keine SAP Produkte sind.

HINWEIS: Es können nur solche Profile an Systemrollen zugewiesen werden, die keiner SAP Rolle zugeordnet sind.

HINWEIS: Gruppen, Rollen und Profile, bei denen die Option **Verwendung nur im IT Shop aktiviert** ist, können nur an Systemrollen zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist. Ausführliche Informationen über die Bereitstellung von Systemrollen im IT Shop finden Sie im One Identity Manager Administrationshandbuch für Systemrollen.

Um eine Gruppe an Systemrollen zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemrollen entfernen.

Um eine Zuweisung zu entfernen

- Wählen Sie die Systemrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Um eine Rolle an Systemrollen zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemrollen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Um ein Profil an Systemrollen zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Profile**.
2. Wählen Sie in der Ergebnisliste das Profil.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemrollen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- SAP Produkte auf Seite 197

Verwandte Themen

- SAP Gruppen, SAP Rollen und SAP Profile an Organisationen zuweisen auf Seite 174
- SAP Gruppen, SAP Rollen und SAP Profile an Geschäftsrollen zuweisen auf Seite 176
- SAP Benutzerkonten direkt an SAP Gruppen und SAP Profile zuweisen auf Seite 178
- SAP Gruppen, SAP Rollen und SAP Profile in den IT Shop aufnehmen auf Seite 182

SAP Gruppen, SAP Rollen und SAP Profile in den IT Shop aufnehmen

HINWEIS: Es können nur solche Profile an IT Shop Regale zugewiesen werden, die keiner SAP Rolle zugeordnet sind.

Mit der Zuweisung einer Gruppe, einer Rolle oder eines Profils an ein IT Shop Regal kann sie von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Die Gruppe, die Rolle oder das Profil muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Gruppe, der Rolle oder dem Profil muss eine Leistungsposition zugeordnet sein.

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Gruppe, die Rolle oder das Profil im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Service-kategorie zu.
- Soll die Gruppe, die Rolle oder das Profil nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss die Gruppe, die Rolle oder das Profil zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen oder Benutzerkonten ist dann nicht mehr zulässig.

HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren Gruppen, Rollen und Profile an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Gruppen, Rollen und Profile in den IT Shop aufzunehmen.

Um eine Gruppe, eine Rolle oder ein Profil in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Gruppen** oder **SAP R/3 | Rollen** oder **SAP R/3 | Profile** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | SAP Gruppen** oder **Berechtigungen | SAP Rollen** oder **Berechtigungen | SAP Profile** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe, die Rolle oder das Profil.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppe, die Rolle oder das Profil an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Gruppe, eine Rolle oder ein Profil aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Gruppen** oder **SAP R/3 | Rollen** oder **SAP R/3 | Profile** (bei nicht-rollenbasierter Anmeldung).

- ODER -

Wählen Sie im Manager die Kategorie **Berechtigungen | SAP Gruppen** oder **Berechtigungen | SAP Rollen** oder **Berechtigungen | SAP Profile** (bei rollenbasierter Anmeldung).

2. Wählen Sie in der Ergebnisliste die Gruppe, die Rolle oder das Profil.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppe, die Rolle oder das Profil aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Gruppe, eine Rolle oder ein Profil aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **SAP R/3 | Gruppen** oder **SAP R/3 | Rollen** oder **SAP R/3 | Profile** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | SAP Gruppen** oder **Berechtigungen | SAP Rollen** oder **Berechtigungen | SAP Profile** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe, die Rolle oder das Profil.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Die Gruppe, die Rolle oder das Profil wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Gruppe, dieser Rolle oder diesem Profil abbestellt.

Ausführliche Informationen zur Bestellung von Unternehmensressourcen über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Verwandte Themen

- Allgemeine Stammdaten von SAP Gruppen auf Seite 169
- SAP Gruppen, SAP Rollen und SAP Profile an Organisationen zuweisen auf Seite 174
- SAP Gruppen, SAP Rollen und SAP Profile an Geschäftsrollen zuweisen auf Seite 176
- SAP Benutzerkonten direkt an SAP Gruppen und SAP Profile zuweisen auf Seite 178
- SAP Gruppen, SAP Rollen und SAP Profile in Systemrollen aufnehmen auf Seite 180

Zuordnung und Vererbung von SAP Profilen und SAP Rollen an SAP Benutzerkonten

Die nachfolgenden SAP-seitigen Einschränkungen beeinflussen die Zuordnung und die Vererbung der Profile und Rollen an Benutzerkonten im One Identity Manager.

- Sammelprofile können aus 0..n Profilen oder Sammelprofilen zusammengesetzt sein. Wird ein Benutzerkonto einem Sammelprofil zugeordnet, so liefert das Zielsystem jeweils nur die Mitgliedschaft des Benutzers im zugeordneten Sammelprofil, jedoch nicht die Mitgliedschaft in untergeordneten Profilen.
- Einzelrollen können aus 0..n Profilen zusammengesetzt sein. Es können nur Profile zugeordnet sein, die keine Sammelprofile sind. Profile, die einer Einzelrolle zugewiesen sind, können nicht mehr an ein Benutzerkonto zugewiesen werden.
- Sammelrollen können aus 0..n Einzelrollen zusammengesetzt sein. Die Zuweisung von Profilen oder Sammelprofilen an Sammelrollen ist nicht möglich.

Aus diesen Einschränkungen ergeben sich folgende Besonderheiten:

In der Zuordnung:

- Die Zuordnung von Profilen, die an Einzelrollen zugewiesen sind, an Benutzerkonten, Systemrollen, hierarchische Rollen und Personen wird per Trigger unterbunden.

Im Vererbungsverhalten:

- Ist einem Benutzerkonto eine Sammelrolle zugeordnet, die Einzelrollen besitzt, dann werden die Einzelrollen nicht in die Tabelle `SAPUserInSAPRole` übernommen.
- Ist einem Benutzerkonto eine Einzelrolle zugeordnet, die Profile besitzt, dann werden die Profile nicht in die Tabelle `SAPUserInSAPProfile` übernommen.
- Ist einem Benutzerkonto eine Einzelrolle zugeordnet und ist diese Einzelrolle Bestandteil einer Sammelrolle, die dem Benutzerkonto ebenfalls zugewiesen ist, dann wird die Einzelrolle nicht in die Tabelle `SAPUserInSAPRole` übernommen.
- Ist einem Benutzerkonto ein Sammelprofil zugeordnet, das untergeordnete Profile besitzt, dann werden die untergeordneten Profile nicht in die Tabelle `SAPUserInSAPProfile` übernommen.

Erhält ein Benutzerkonto Rollen oder Profile zusätzlich über einen Referenzbenutzer, dann werden diese Rollen oder Profile nur für den Referenzbenutzer in die Tabellen `SAPUserInSAPRole` und `SAPUserInSAPProfile` übernommen. Bei der Berechnung der Unternehmensressourcen, die einer Person zugewiesen sind (Tabelle `PersonHasObject`), werden auch die Rollen und Profile berücksichtigt, die ein Benutzerkonto über Einzelrollen, Sammelrollen, Sammelprofile und Referenzbenutzer erbt.

Zusätzliche Aufgaben zur Verwaltung der SAP Gruppen, SAP Rollen und SAP Profile

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Überblick über die SAP Gruppen, SAP Rollen und SAP Profile

Um einen Überblick über eine Gruppe zu erhalten

1. Wählen Sie die Kategorie **SAP R/3 | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die SAP Gruppe**.

Um einen Überblick über ein Profil zu erhalten

1. Wählen Sie die Kategorie **SAP R/3 | Profile**.
2. Wählen Sie in der Ergebnisliste das Profil.
3. Wählen Sie die Aufgabe **Überblick über das SAP Profil**.

Um einen Überblick über eine Rolle zu erhalten

1. Wählen Sie die Kategorie **SAP R/3 | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Überblick über die SAP Rolle**.

Wirksamkeit von SAP Gruppen, SAP Rollen und SAP Profilen

HINWEIS: Für ein leichteres Verständnis ist in diesem Abschnitt das Verhalten anhand der SAP Gruppen beschrieben. Es gilt gleichermaßen für Rollen und Profile.

Tabelle 66: Konfigurationsparameter für die bedingte Vererbung

Konfigurationsparameter	Wirkung bei Aktivierung
QER | Structures | Inherite | GroupExclusion	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Wirksamkeit von Gruppenmitgliedschaften. Ist der Parameter aktiviert, können aufgrund von Ausschlussdefinitionen die Gruppenmitgliedschaften reduziert werden. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.

Bei der Zuweisung von Gruppen an Benutzerkonten kann es vorkommen, dass eine Person zwei oder mehr Gruppen erhält, die in dieser Kombination nicht auftreten dürfen. Um das zu verhindern, geben Sie die sich ausschließenden Gruppen bekannt. Dabei legen Sie für zwei Gruppen fest, welche der beiden Gruppen an Benutzerkonten wirksam werden soll, wenn beide zugewiesen sind.

Die Zuweisung einer ausgeschlossenen Gruppe ist jederzeit direkt, indirekt oder per IT Shop-Bestellung möglich. Anschließend ermittelt der One Identity Manager, ob diese Zuweisung wirksam ist.

HINWEIS:

- Ein wechselseitiger Ausschluss zweier Gruppen kann nicht definiert werden. Das heißt, die Festlegung "Gruppe A schließt Gruppe B aus" UND "Gruppe B schließt Gruppe A aus" ist nicht zulässig.
- Für eine Gruppe muss jede auszuschließende Gruppe einzeln bekannt gegeben werden. Ausschlussdefinitionen werden nicht vererbt.

Die Wirksamkeit der Zuweisungen wird in den Tabellen SAPUserInSAPGrp und BaseTreeHasSAPGrp über die Spalte XIsInEffect abgebildet.

Beispiel für die Wirksamkeit von Gruppenmitgliedschaften

- In einem Mandanten ist eine Gruppe A mit Berechtigungen zum Auslösen von Bestellungen definiert. Eine Gruppe B berechtigt zum Anweisen von Zahlungen. Eine Gruppe C berechtigt zum Prüfen von Rechnungen.
- Gruppe A wird über die Abteilung "Marketing", Gruppe B über die Abteilung "Finanzen" und Gruppe C wird über die Geschäftsrolle "Kontrollgruppe" zugewiesen.

Clara Harris hat ein Benutzerkonto in diesem Mandanten. Sie gehört primär der Abteilung "Marketing" an. Sekundär sind ihr die Geschäftsrolle "Kontrollgruppe" und die Abteilung "Finanzen" zugewiesen. Ohne Ausschlussdefinition erhält das Benutzerkonto alle Berechtigungen der Gruppen A, B und C.

Durch geeignete Maßnahmen soll verhindert werden, dass eine Person sowohl Bestellungen auslösen als auch Rechnungen zur Zahlung anweisen kann. Das heißt,

die Gruppen A und B schließen sich aus. Eine Person, die Rechnungen prüft, darf ebenfalls keine Rechnungen zur Zahlung anweisen. Das heißt, die Gruppen B und C schließen sich aus.

Tabelle 67: Festlegen der ausgeschlossenen Gruppen (Tabelle `SAPGrpExclusion`)

Wirksame Gruppe	Ausgeschlossene Gruppe
Gruppe A	
Gruppe B	Gruppe A
Gruppe C	Gruppe B

Tabelle 68: Wirksame Zuweisungen

Person	Mitglied in Rolle	Wirksame Gruppe
Ben King	Marketing	Gruppe A
Jan Bloggs	Marketing, Finanzen	Gruppe B
Clara Harris	Marketing, Finanzen, Kontrollgruppe	Gruppe C
Jenny Basset	Marketing, Kontrollgruppe	Gruppe A, Gruppe C

Für Clara Harris ist nur die Zuweisung der Gruppe C wirksam und wird ins Zielsystem publiziert. Verlässt Clara Harris die Geschäftsrolle "Kontrollgruppe" zu einem späteren Zeitpunkt, wird die Gruppe B ebenfalls wirksam.

Für Jenny Basset sind die Gruppen A und C wirksam, da zwischen beiden Gruppen kein Ausschluss definiert wurde. Soll das verhindert werden, definieren Sie einen weiteren Ausschluss für die Gruppe C.

Tabelle 69: Ausgeschlossene Gruppen und wirksame Zuweisungen

Person	Mitglied in Rolle	Zugewiesene Gruppe	Ausgeschlossene Gruppe	Wirksame Gruppe
Jenny Basset	Marketing	Gruppe A		Gruppe C
	Kontrollgruppe	Gruppe C	Gruppe B Gruppe A	

Voraussetzungen

- Der Konfigurationsparameter "QER\Structures\Inherite\GroupExclusion" ist aktiviert.
- Sich ausschließende Gruppen, Rollen und Profile gehören zum selben Mandanten.

Um Gruppen auszuschließen

1. Wählen Sie die Kategorie **SAP R/3 | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppen ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu, die sich mit der gewählten Gruppe ausschließen.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Um Rollen auszuschließen

1. Wählen Sie die Kategorie **SAP R/3 | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **SAP Rollen ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Rollen zu, die sich mit der gewählten Rolle ausschließen.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Rollen, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Um Profile auszuschließen

1. Wählen Sie die Kategorie **SAP R/3 | Profile**.
2. Wählen Sie in der Ergebnisliste das Profil.
3. Wählen Sie die Aufgabe **Profile ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Profile zu, die sich mit dem gewählten Profil ausschließen.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Profile, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Vererbung von SAP Gruppen, SAP Rollen und SAP Profilen anhand von Kategorien

HINWEIS: Für ein leichteres Verständnis ist in diesem Abschnitt das Verhalten anhand der SAP Gruppen beschrieben. Es gilt gleichermaßen für Rollen und Profile.

Im One Identity Manager können Gruppen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält verschiedene Tabellen. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In den übrigen Tabellen geben Sie Ihre Kategorien für die zielsystemabhängigen Gruppen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 31**.

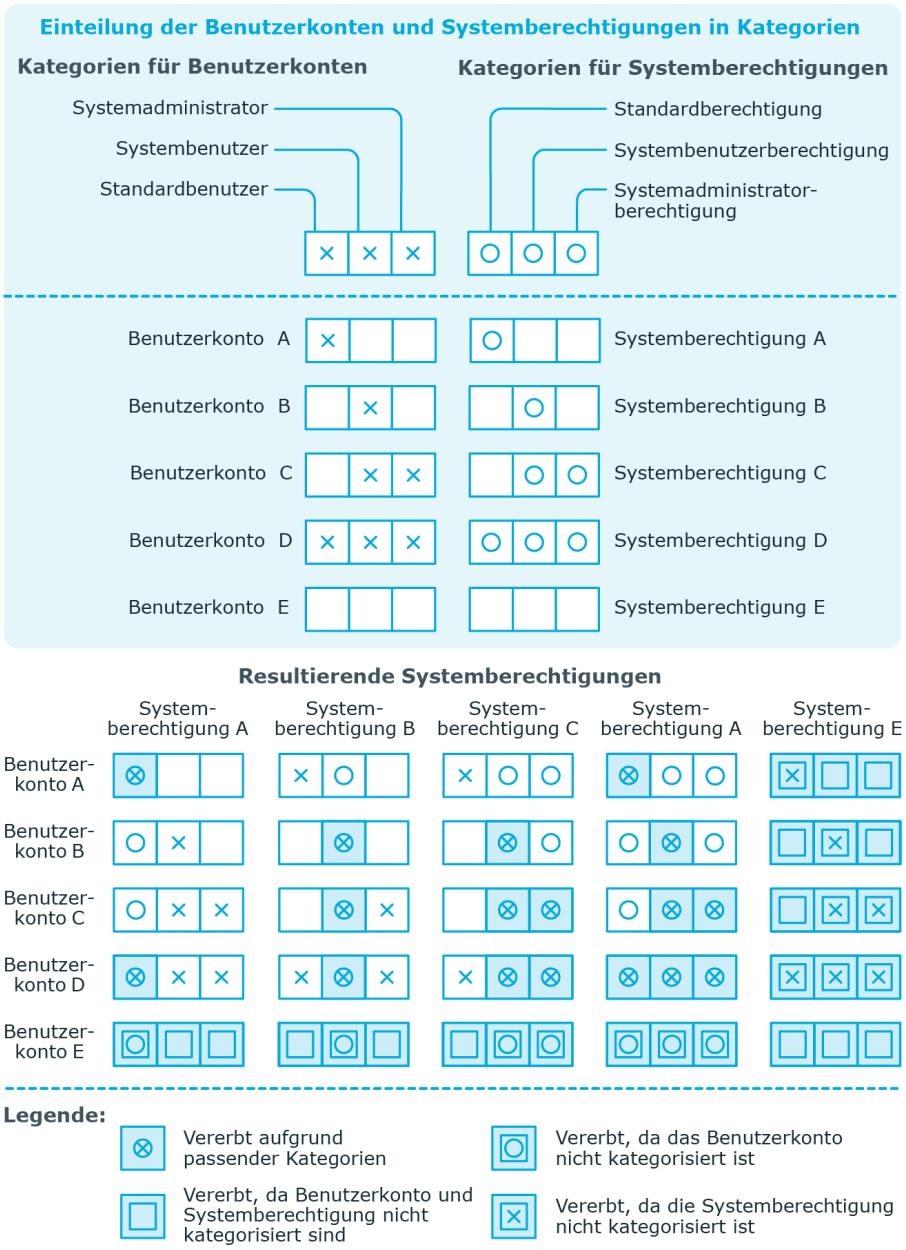
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto vererbt. Ist die Gruppe oder das Benutzerkonto nicht in Kategorien eingestuft, dann wird die Gruppe ebenfalls an das Benutzerkonto vererbt.

HINWEIS: Die Vererbung über Kategorien wird nur bei der indirekten Zuweisung von Gruppen über hierarchische Rollen berücksichtigt. Bei der direkten Zuweisung von Gruppen an Benutzerkonten werden die Kategorien nicht berücksichtigt.

Tabelle 70: Beispiele für Kategorien

Kategorieposition	Kategorien für Benutzerkonten	Kategorien für Gruppen
1	Standardbenutzer	Standardberechtigung
2	Systembenutzer	Systembenutzerberechtigung
3	Systemadministrator	Systemadministratorberechtigung

Abbildung 5: Beispiel für die Vererbung über Kategorien



Um die Vererbung über Kategorien zu nutzen

- Definieren Sie am Mandanten die Kategorien.
  HINWEIS: Wenn eine Zentrale Benutzerverwaltung eingesetzt wird, definieren Sie die Kategorien sowohl am Zentralsystem als auch an den Tochtersystemen. Damit Gruppen aus einem Tochtersystem an Benutzerkonten vererbt werden können, müssen an den Tochtersystemen die selben Kategorien definiert sein wie am Zentralsystem.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.

- Weisen Sie die Kategorien den Gruppen, Rollen und Profilen über ihre Stammdaten zu.

Verwandte Themen

- Festlegen der Kategorien für die Vererbung von SAP Gruppen, SAP Rollen und SAP Profilen auf Seite 125
- Allgemeine Stammdaten eines SAP Benutzerkontos auf Seite 136
- Allgemeine Stammdaten von SAP Gruppen auf Seite 169
- Allgemeine Stammdaten von SAP Rollen auf Seite 170
- Allgemeine Stammdaten von SAP Profilen auf Seite 171

Zusatzeigenschaften an SAP Gruppen, SAP Rollen und SAP Profile zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

Um Zusatzeigenschaften für eine Gruppe festzulegen

1. Wählen Sie die Kategorie **SAP R/3 | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Zusatzeigenschaften.
5. Speichern Sie die Änderungen.

Um Zusatzeigenschaften für eine Rolle festzulegen

1. Wählen Sie die Kategorie **SAP R/3 | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Zusatzeigenschaften.
5. Speichern Sie die Änderungen.

Um Zusatzeigenschaften für ein Profil festzulegen

1. Wählen Sie die Kategorie **SAP R/3 | Profile**.
2. Wählen Sie in der Ergebnisliste das Profil.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Zusatzeigenschaften.
5. Speichern Sie die Änderungen.

SAP Berechtigungen anzeigen

Im One Identity Manager können Sie die Berechtigungen und Berechtigungsobjekte der SAP Rollen und Profile anzeigen. Dabei wird eine hierarchische Übersicht aller Einzelprofile mit den zugehörigen Berechtigungsobjekten und Berechtigungsfeldern angezeigt.

Um Berechtigungen für eine Rolle anzuzeigen

1. Wählen Sie die Kategorie **SAP R/3 | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **SAP Berechtigungen anzeigen**.

Um Berechtigungen für ein Profil anzuzeigen

1. Wählen Sie die Kategorie **SAP R/3 | Profile**.
2. Wählen Sie in der Ergebnisliste das Profil.
3. Wählen Sie die Aufgabe **SAP Berechtigungen anzeigen**.

Gültigkeitszeitraum von Rollenzuweisungen

Für die Zuweisung von SAP Rollen an Benutzerkonten kann ein Gültigkeitszeitraum angegeben werden. Wenn kein Gültigkeitszeitraum angegeben ist, erhalten Rollenzuweisungen standardmäßig folgende Gültigkeitsdaten:

- Gültig von: **1900-01-01**
- Gültig bis: **9999-12-31**

Diese Rollenzuweisungen sind damit unbefristet.

Die Tabelle `SAPUserInSAPRole` enthält alle Rollenzuweisungen, sowohl unbefristete, als auch alle befristeten.

Die Tabelle HelperSAPUserInSAPRole enthält nur die aktuell gültigen Rollenzuweisungen. Die Berechnung dieser Tabelle wird durch den Zeitplan **Tägliche Neuberechnung der Zuweisungen von SAP Benutzerkonten an SAP Rollen** gesteuert.

Detaillierte Informationen zum Thema

- Gültigkeitszeitraum direkter Rollenzuweisungen auf Seite 193
- Gültigkeitszeitraum indirekter Rollenzuweisungen konfigurieren auf Seite 193
- Gültigkeitszeitraum indirekter Rollenzuweisungen ermitteln auf Seite 195

Verwandte Themen

- SAP Rollen direkt an ein SAP Benutzerkonto zuweisen auf Seite 149
- SAP Benutzerkonten direkt an SAP Rollen zuweisen auf Seite 179

Gültigkeitszeitraum direkter Rollenzuweisungen

Direktzuweisungen können auf zwei Wegen entstehen:

a. Synchronisation von Rollenzuweisungen

   Im Standardmapping sind die Spalten **Gültig von** und **Gültig bis** berücksichtigt. Die Synchronisation schreibt den Gültigkeitszeitraum von Rollenzuweisungen in die One Identity Manager-Datenbank.

b. Direktzuweisung von SAP Rollen an Benutzerkonten im Manager

   Bei der direkten Zuweisung von SAP Rollen an Benutzerkonten kann ein Gültigkeitszeitraum erfasst werden. **Gültig von**- und **Gültig bis**-Datum werden in das Zielsystem provisioniert.

Verwandte Themen

- Gültigkeitszeitraum indirekter Rollenzuweisungen ermitteln auf Seite 195
- Gültigkeitszeitraum von Rollenzuweisungen auf Seite 192

Gültigkeitszeitraum indirekter Rollenzuweisungen konfigurieren

Bei der Ermittlung des Gültigkeitszeitraums werden die folgenden Konfigurationsparameter ausgewertet. Die Konfigurationsparameter sind standardmäßig deaktiviert.

- **TargetSystem | SAPR3 | ValidDateHandling | DoNotUsePWODate**

  Legt fest, ob bei der Bestellung von Rollenzuweisungen der Gültigkeitszeitraum der Bestellung übernommen wird.

  Nicht aktiviert: Der Gültigkeitszeitraum der Bestellung wird übernommen. Ist kein Gültigkeitszeitraum angegeben, werden die Standardwerte **1900-01-01** und **9999-12-31** gesetzt.

  Aktiviert: Die Rollenzuweisung ist unbefristet.

- **TargetSystem | SAPR3 | ValidDateHandling | ReuseInheritedDate**

  Steuert die Nachnutzung von bereits vorhandenen Rollenzuweisungen, wenn eine weitere Zuweisung für dieselbe Kombination aus Benutzerkonto und SAP Rolle eingefügt wird.

  Aktiviert: Bereits vorhandene Rollenzuweisungen werden nachgenutzt, wenn dieselbe Zuweisung über verschiedene Vererbungswege entsteht. Dabei gilt:

  - Das **Gültig von**-Datum der vorhandenen Zuweisung liegt in der Vergangenheit.
  - Das **Gültig bis**-Datum der vorhandenen Zuweisung ist **9999-12-31** oder die neu hinzukommende Zuweisung hat dasselbe **Gültig bis**-Datum, wie die bereits vorhandene Zuweisung.

  Für jede weitere unbefristete Zuweisung und für jede weitere Zuweisung mit demselben **Gültig bis**-Datum wird kein neuer Eintrag in der Tabelle `SAPUserInSAPRole` erzeugt. Dadurch kann die Anzahl der Einträge in der Tabelle `SAPUserInSAPRole` reduziert werden.

  Nicht aktiviert: Für jede neue Rollenzuweisung wird ein neuer Eintrag in der Tabelle `SAPUserInSAPRole` erzeugt. Bestehende Zuweisungen werden nicht nachgenutzt.

  > HINWEIS: In Datenbanken, die aus einer Version älter als 7.0 migriert wurden, kann es Zuweisungen mit dem **Gültig bis**-Datum **9998-12-31** geben. Das ist ein gültiger Wert für unbefristete Rollenzuweisungen, sodass diese Zuweisungen ebenfalls nachgenutzt werden.

- **TargetSystem | SAPR3 | ValidDateHandling | ReuseInheritedDate | UseTodayForInheritedValidFrom**

  Legt fest, welchen Wert das **Gültig von**-Datum indirekter Rollenzuweisungen bei Neuanlage erhält.

  Nicht aktiviert: **1900-01-01**

  Aktiviert: **<Heute>**

  > WICHTIG: Abhängig von der Menge der zu verarbeitenden Daten kann die Berechnung der indirekten Rollenzuweisungen dadurch deutlich verlangsamt werden.
  >
  > Lassen Sie den Konfigurationsparameter deaktiviert, wenn die Information, seit wann die Rollenzuweisung gültig ist, in der SAP R/3-Umgebung nicht zwingend benötigt wird.

Um bestehende Rollenzuweisungen nachzunutzen

- Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | SAPR3 | ValidDateHandling | ReuseInheritedDate**.

Um das Datum der Zuweisung als ersten Gültigkeitstag der Rollenzuweisung zu setzen

- Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | SAPR3 | ValidDateHandling | ReuseInheritedDate | UseTodayForInheritedValidFrom**.

Um zu verhindern, dass der Gültigkeitszeitraum der Bestellung an die Rollenzuweisung übernommen wird

- Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | SAPR3 | ValidDateHandling | DoNotUsePWODate**.

  Es wird eine unbefristete Rollenzuweisung angelegt.

Verwandte Themen

- Gültigkeitszeitraum indirekter Rollenzuweisungen ermitteln auf Seite 195

Gültigkeitszeitraum indirekter Rollenzuweisungen ermitteln

SAP Rollen, die an Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen zugewiesen sind, werden dadurch indirekt an die Benutzerkonten zugewiesen. Indirekte Zuweisungen sind standardmäßig unbefristet. Für die Ermittlung des Gültigkeitszeitraums indirekter Zuweisungen werden die Konfigurationsparameter unter **TargetSystem | SAPR3 | ValidDateHandling** ausgewertet.

Bei Bestellungen im IT Shop kann ein Gültigkeitszeitraum für die Bestellung angegeben werden. Ein Eintrag in der Tabelle `SAPUserInSAPRole` existiert nur zwischen dem ersten und letzten Gültigkeitstag der Bestellung. Der Gültigkeitszeitraum der Bestellung wird unter folgenden Voraussetzungen an die Rollenzuweisungen übernommen:

- Der Konfigurationsparameter **DoNotUsePWODate** ist deaktiviert (Standard).
- Die SAP Rolle wurde direkt bestellt.

  - ODER -

- Die Zuweisung ist über eine Zuweisungsbestellung entstanden. Dabei wurde eine Zuweisung an Rollen bestellt. Für diese ist `BaseTreeHasSAPRole.XOrigin='8'` gesetzt

Standardmäßig wird für jede neue Rollenzuweisung ein neuer Eintrag in der Tabelle `SAPUserInSAPRole` erzeugt. Entsteht dieselbe Zuweisung über verschiedene Vererbungswege, kann die Zahl der Einträge in der Tabelle `SAPUserInSAPRole` schnell anwachsen. Für diesen Fall können bestehende Einträge nachgenutzt werden, wenn der

Gültigkeitszeitraum identisch ist. Bereits vorhandene Rollenzuweisungen werden unter folgenden Voraussetzungen nachgenutzt:

- Der Konfigurationsparameter **ReuseInheritedDate** ist aktiviert.
- Das **Gültig von**-Datum der vorhandenen Zuweisung liegt in der Vergangenheit.
- Das **Gültig bis**-Datum der vorhandenen Zuweisung ist **9999-12-31** oder die neu hinzukommende Zuweisung hat dasselbe **Gültig bis**-Datum, wie die bereits vorhandene Zuweisung.
- Es wird eine weitere Zuweisung für dieselbe Kombination aus Benutzerkonto und SAP Rolle eingefügt.

Für jede weitere unbefristete Zuweisung und für jede weitere Zuweisung mit demselben **Gültig bis**-Datum wird kein neuer Eintrag in der Tabelle `SAPUserInSAPRole` erzeugt. Die Anzahl der Einträge in der Tabelle `SAPUserInSAPRole` kann dadurch reduziert werden.

HINWEIS: In Datenbanken, die aus einer Version älter als 7.0 migriert wurden, kann es Zuweisungen mit dem **Gültig bis**-Datum **9998-12-31** geben. Das ist ein gültiger Wert für unbefristete Rollenzuweisungen, sodass diese Zuweisungen ebenfalls nachgenutzt werden.

Der erste Gültigkeitstag indirekter Zuweisungen ist standardmäßig **1900-01-01**. Damit ist nicht ersichtlich, wann die Zuweisung entstanden ist. Wenn diese Information benötigt wird, kann an das **Gültig von**-Datum das aktuelle Datum eingetragen werden, an dem die SAP Rolle zugewiesen wird. Das Datum der Zuweisung wird unter folgenden Voraussetzungen als erster Gültigkeitstag indirekter Rollenzuweisungen gesetzt:

- Der Konfigurationsparameter **ReuseInheritedDate | UseTodayForInheritedValidFrom** ist aktiviert.

  Ausnahmen: Der Konfigurationsparameter **DoNotUsePWODate** ist deaktiviert und
  - die Zuweisung wurde bestellt und an der Bestellung ist ein **Gültig von**-Datum angegeben.
  - die Zuweisung wurde bestellt und an der Bestellung ist ein **Gültig bis**- aber kein **Gültig von**-Datum angegeben.

WICHTIG: Abhängig von der Menge der zu verarbeitenden Daten kann die Berechnung der indirekten Rollenzuweisungen dadurch deutlich verlangsamt werden.

Lassen Sie den Konfigurationsparameter **UseTodayForInheritedValidFrom** deaktiviert, wenn die Information, seit wann die Rollenzuweisung gültig ist, in der SAP R/3-Umgebung nicht zwingend benötigt wird.

Detaillierte Informationen zum Thema

- Gültigkeitszeitraum indirekter Rollenzuweisungen konfigurieren auf Seite 193
- Gültigkeitszeitraum von Rollenzuweisungen auf Seite 192

Verwandte Themen

- Gültigkeitszeitraum direkter Rollenzuweisungen auf Seite 193

9

SAP Produkte

Installierte Module: Systemrollenmodul

Im One Identity Manager können Sie SAP Produkte als Zusammenstellung von verschiedenen Gruppen, Rollen oder Profilen definieren. SAP Produkte sind Systemrollen mit dem Systemrollentyp "SAP Produkt". Personen können SAP Produkte direkt erhalten, über hierarchische Rolle erben oder im IT Shop bestellen.

Unabhängig vom Weg der Zuweisung werden dem Benutzerkonto einer Person die Gruppen, Rollen und Profile zugewiesen, die im SAP Produkt enthalten sind. Wird ein SAP Produkt im One Identity Manager durch Hinzufügen oder Entfernen einer Gruppe, einer Rolle oder eines Profils verändert, so werden die Mitgliedschaften der Benutzerkonten entsprechend angepasst.

Um SAP Produkte zu bearbeiten

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste ein SAP Produkt.

   – ODER –

   Klicken Sie in der Ergebnisliste .

   Das Stammdatenformular einer Systemrolle wird geöffnet.
3. Bearbeiten Sie die Stammdaten der Systemrolle.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- One Identity Manager Administrationshandbuch für Systemrollen

Allgemeine Stammdaten eines SAP Produkts

Tabelle 71: Konfigurationsparameter für die Risikobewertung von SAP Benutzerkonten

Konfigurationsparameter	Wirkung bei Aktivierung
QER\CalculateRiskIndex	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Berechnung des Risikoindex. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Werte für den Risikoindex erfasst und berechnet werden.

Für Systemrollen erfassen Sie folgende Stammdaten.

Tabelle 72: Stammdaten einer Systemrolle

Eigenschaft	Beschreibung
Anzeigename	Bezeichnung unter der die Systemrolle in den Werkzeugen des One Identity Manager angezeigt werden soll.
Systemrolle	Eindeutige Bezeichnung für die Systemrolle.
Interner Produktname	Zusätzliche interne Bezeichnung für die Systemrolle.
Systemrollentyp	Gibt an, welcher Art Unternehmensressourcen in der Systemrolle zusammengefasst werden.
Leistungsposition	Um eine Systemrolle innerhalb des IT Shops zu verwenden, weisen Sie ihr eine Leistungsposition zu oder legen Sie eine neue Leistungsposition an. Ausführliche Informationen über Leistungspositionen finden Sie im One Identity Manager Administrationshandbuch für IT Shop.
Verantwortlicher der Systemrolle	Verantwortlicher für die Systemrolle. Ordnen Sie eine beliebige Person zu. Diese Person kann die Stammdaten der Systemrolle bearbeiten. Sie kann als Attestierer für die Eigenschaften der Systemrolle ermittelt werden. Wenn die Systemrolle im IT Shop bestellt werden kann, wird der Verantwortliche automatisch Mitglied in der Anwendungsrolle für Produkteigner, die der Leistungsposition zugeordnet ist.
Freigabedatum	Legen Sie einen Zeitpunkt fest, an dem die Systemrolle aktiviert werden soll. Liegt das Freigabedatum in der Zukunft, wird die Systemrolle als deaktivierte Systemrolle behandelt. Ist das Freigabedatum

Eigenschaft	Beschreibung
	erreicht wird die Systemrolle aktiviert. Unternehmensressourcen, die der Systemrolle zugewiesen sind, werden an Personen vererbt. Ist das Freigabedatum überschritten oder ist kein Datum eingetragen, wird die Systemrolle als aktivierte Systemrolle behandelt. Die Vererbung der Unternehmensressourcen kann in diesen Fällen über die Option **Deaktiviert** gesteuert werden. HINWEIS: Konfigurieren und aktivieren Sie im Designer den Zeitplan **Systemrollen freigeben**, um das Freigabedatum zu überprüfen. Ausführliche Informationen zu Zeitplänen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten Unternehmensressourcen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen zur Berechnung des Risikoindex finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kommentar	Freitextfeld für zusätzliche Erläuterungen.
Bemerkungen	Freitextfeld für zusätzliche Erläuterungen.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Deaktiviert	Angabe, ob die Unternehmensressourcen, die in der Systemrolle zusammengefasst sind, an Personen und Arbeitsplätze vererbt werden. Ist die Option aktiviert, kann die Systemrolle an Personen, Arbeitsplätze, hierarchische Rollen und IT Shop Regale zugewiesen werden. Die enthaltenen Unternehmensressourcen werden jedoch nicht vererbt. Die Systemrolle kann nicht im Web Portal bestellt werden. Ist die Option deaktiviert, werden die Unternehmensressourcen, die der Systemrolle zugewiesen sind, vererbt. Wird die Option zu einem späteren Zeitpunkt aktiviert, werden bestehende Zuweisungen entfernt.
IT Shop	Angabe, ob die Systemrolle über den IT Shop bestellbar ist. Die Systemrolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Systemrolle kann weiterhin direkt an Personen und hierarchische Rollen zugewiesen werden. Ausführliche Informationen über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.
Verwendung im	Angabe, ob die Systemrolle ausschließlich über den IT Shop bestellbar

Eigenschaft	Beschreibung
IT Shop	ist. Die Systemrolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Systemrolle an hierarchische Rollen ist nicht zulässig.
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Ausführliche Informationen über Systemrollen finden Sie im *One Identity Manager Administrationshandbuch für Systemrollen*.

SAP Produkte an Personen zuweisen

SAP Produkte können direkt oder indirekt an Personen zugewiesen werden. Bei der indirekten Zuweisung werden Personen und SAP Produkte in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der SAP Produkte, die einer Person zugewiesen ist.

Wenn Sie eine Person in hierarchische Rollen aufnehmen und die Person ein Benutzerkonto besitzt, dann wird dieses Benutzerkonto in alle Gruppen, Rollen und Profile aufgenommen, die in den SAP Produkten zusammengefasst sind, welche die Person besitzt. Ist das SAP Produkt deaktiviert oder liegt das Freigabedatum in der Zukunft, werden die Gruppen, Rollen und Profile nicht vererbt.

Voraussetzungen für die indirekte Zuweisung sind:

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Systemrollen, Personen, Gruppen, Rollen und Profilen erlaubt.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.
- Die Benutzerkonten, Gruppen, Rollen und Profile gehören zum selben SAP Mandanten.

Des Weiteren können SAP Produkte über IT Shop-Bestellungen an Personen zugewiesen werden. Damit SAP Produkte über IT Shop-Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle SAP Produkte, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte SAP Produkte werden nach erfolgreicher Genehmigung den Personen zugewiesen.

Detaillierte Informationen zum Thema

- SAP Produkte an Organisationen zuweisen auf Seite 201
- SAP Produkte an Geschäftsrollen zuweisen auf Seite 201
- SAP Produkte direkt an Personen zuweisen auf Seite 202
- SAP Produkte in Systemrollen aufnehmen auf Seite 203

- SAP Produkte in den IT Shop aufnehmen auf Seite 204
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

Verwandte Themen

- SAP Gruppen, SAP Rollen und SAP Profile an SAP Benutzerkonten zuweisen auf Seite 173

SAP Produkte an Organisationen zuweisen

Weisen Sie SAP Produkte an Abteilungen, Kostenstellen oder Standorte zu, damit sie über diese Organisationen an Personen zugewiesen werden.

Um ein SAP Produkt an Abteilungen, Kostenstellen oder Standorte zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
    - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
    - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
    - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

    - ODER -

    Entfernen Sie im Bereich **Zuordnungen entfernen** die Organisationen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Produkte an Geschäftsrollen zuweisen auf Seite 201
- SAP Produkte in den IT Shop aufnehmen auf Seite 204
- SAP Produkte direkt an Personen zuweisen auf Seite 202
- SAP Produkte in Systemrollen aufnehmen auf Seite 203
- SAP Gruppen, SAP Rollen und SAP Profile an Organisationen zuweisen auf Seite 174

SAP Produkte an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie SAP Produkte an Geschäftsrollen zu, damit sie über diese Geschäftsrollen an Personen zugewiesen werden.

Um ein SAP Produkt an Geschäftsrollen zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Produkte an Organisationen zuweisen
- SAP Produkte in Systemrollen aufnehmen auf Seite 203
- SAP Produkte direkt an Personen zuweisen auf Seite 202
- SAP Produkte in den IT Shop aufnehmen auf Seite 204
- SAP Gruppen, SAP Rollen und SAP Profile an Geschäftsrollen zuweisen auf Seite 176

SAP Produkte direkt an Personen zuweisen

Sie können SAP Produkte direkt an Personen zuweisen. Alle Gruppen, Rollen und Profile, die dem SAP Produkt zugewiesen sind, werden an diese Personen vererbt.

Um ein SAP Produkt direkt an Personen zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt.
3. Wählen Sie die Aufgabe **An Personen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Personen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Produkte an Organisationen zuweisen auf Seite 201
- SAP Produkte an Geschäftsrollen zuweisen auf Seite 201

- SAP Produkte in den IT Shop aufnehmen auf Seite 204
- SAP Produkte in Systemrollen aufnehmen auf Seite 203

SAP Produkte in Systemrollen aufnehmen

Sie können verschiedene SAP Produkte zu einem Paket zusammenfassen. Dazu weisen Sie die SAP Produkte an Systemrollen zu.

HINWEIS: SAP Produkte, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können nur an Systemrollen zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist.

Um ein SAP Produkt an Systemrollen zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Wählen Sie den Tabreiter **Systemrolle ist enthalten in**, um übergeordnete Systemrollen zuzuweisen.
    - Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

      - ODER -

      Entfernen Sie im Bereich **Zuordnungen entfernen** die Systemrollen.
5. Wählen Sie den Tabreiter **Systemrolle enthält**, um untergeordnete Systemrolle zuzuweisen.
    - Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

      - ODER -

      Entfernen Sie im Bereich **Zuordnungen entfernen** die Systemrollen.
6. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Produkte an Organisationen zuweisen auf Seite 201
- SAP Produkte an Geschäftsrollen zuweisen auf Seite 201
- SAP Produkte direkt an Personen zuweisen auf Seite 202
- SAP Produkte in den IT Shop aufnehmen auf Seite 204
- SAP Gruppen, SAP Rollen und SAP Profile in Systemrollen aufnehmen auf Seite 180

SAP Produkte in den IT Shop aufnehmen

Mit der Zuweisung eines SAP Produkts an ein IT Shop Regal kann es von den Kunden des Shops bestellt werden. Für die Bestellbarkeit eines SAP Produkts sind weitere Voraussetzungen zu gewährleisten.

- Das SAP Produkt muss mit der Option **IT Shop** gekennzeichnet sein.
- Dem SAP Produkt muss eine Leistungsposition zugeordnet sein.
- Soll das SAP Produkt nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss das SAP Produkt zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung des SAP Produkts an hierarchische Rollen ist dann nicht mehr zulässig.

Um ein SAP Produkt in den IT Shop aufzunehmen

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** das SAP Produkt an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um ein SAP Produkt aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** das SAP Produkt aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um ein SAP Produkt aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Das SAP Produkt wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit diesem SAP Produkt abbestellt.

Ausführliche Informationen über die Bereitstellung von Produkten im IT Shop finden Sie im One Identity Manager Administrationshandbuch für IT Shop.

Verwandte Themen

- SAP Produkte direkt an Personen zuweisen auf Seite 202
- SAP Produkte an Organisationen zuweisen auf Seite 201
- SAP Produkte in Systemrollen aufnehmen auf Seite 203
- SAP Produkte an Geschäftsrollen zuweisen auf Seite 201
- SAP Gruppen, SAP Rollen und SAP Profile in den IT Shop aufnehmen auf Seite 182

Zusätzliche Aufgaben zur Verwaltung von SAP Produkten

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Überblick über das SAP Produkt

Um einen Überblick über ein SAP Produkt zu erhalten

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt.
3. Wählen Sie die Aufgabe **Überblick über die Systemrolle**.

SAP Gruppen, SAP Rollen und SAP Profile an ein SAP Produkt zuweisen

Weisen Sie dem SAP Produkt die Gruppen, Rollen und Profile zu, die Sie zusammenfassen wollen. Wenn Sie das SAP Produkt an Personen zuweisen, werden diese Gruppen, Rollen und Profile an die Person vererbt.

HINWEIS: Gruppen, Rollen und Profile, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können nur an SAP Produkte zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist.

HINWEIS: Gruppen, Rollen und Profile können auch in Systemrollen aufgenommen werden, die keine SAP Produkte sind.

Um Gruppen an ein SAP Produkt zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt.
3. Wählen Sie die Aufgabe **SAP Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
5. Speichern Sie die Änderungen.

Um Profile an ein SAP Produkt zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt.
3. Wählen Sie die Aufgabe **SAP Profile zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Profile zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Profile.
5. Speichern Sie die Änderungen.

Um Rollen an ein SAP Produkt zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt.
3. Wählen Sie die Aufgabe **SAP Rollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Rollen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Rollen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- SAP Produkte an Personen zuweisen auf Seite 200

Kontendefinitionen an ein SAP Produkt zuweisen

Mit dieser Aufgabe nehmen Sie Kontendefinitionen in das SAP Produkt auf. Wenn Sie das SAP Produkt an Personen zuweisen, werden die Kontendefinitionen, die in diesem SAP Produkt enthalten sind, an die Personen vererbt.

HINWEIS: Kontendefinitionen, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können nur an SAP Produkte zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist.

Um Kontendefinitionen an ein SAP Produkt zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt.
3. Wählen Sie die Aufgabe **Kontendefinitionen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontendefinitionen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Kontendefinitionen.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Einrichten von Kontendefinitionen

Abonnierbare Berichte an ein SAP Produkt zuweisen

Installierte Module: Modul Berichtsabonnement

Mit dieser Aufgabe nehmen Sie abonnierbare Berichte in das SAP Produkt auf. Wenn Sie das SAP Produkt an Personen zuweisen, werden die abonnierbaren Berichte, die in diesem SAP Produkt enthalten sind, an die Personen vererbt.

HINWEIS: Abonnierbare Berichte, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können nur an SAP Produkte zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist.

Um abonnierbare Berichte an ein SAP Produkt zuzuweisen

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt.
3. Wählen Sie die Aufgabe **Abonnierbare Berichte zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die abonnierbare Berichte zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die abonnierbare Berichte.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- One Identity Manager Administrationshandbuch für Berichtsabonnements

Zusatzeigenschaften an ein SAP Produkt zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

Um Zusatzeigenschaften für ein SAP Produkt festzulegen

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Zusatzeigenschaften.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Zusatzeigenschaften an SAP Gruppen, SAP Rollen und SAP Profile zuweisen auf Seite 191

Widersprechende Systemrollen bearbeiten

Tabelle 73: Konfigurationsparameter für die Bearbeitung sich ausschließender Rollen

Konfigurationsparameter	Wirkung bei Aktivierung
QER\Structures\Inherite\ESetExclusion	Präprozessorrelevanter Konfigurationsparameter zur Definition der Wirksamkeit von Systemrollen. Ist der Parameter aktiviert, können sich ausschließende Systemrollen definiert werden. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.

Es kann erforderlich sein, dass Personen bestimmte Gruppen, Rollen und Profile nicht gleichzeitig besitzen dürfen. Um das zu verhindern, können Sie die sich gegenseitig

ausschließenden Gruppen, Rollen und Profile an verschiedene SAP Produkte zuweisen. Diese SAP Produkte definieren Sie anschließend als widersprechende Systemrollen. Widersprechende Systemrollen können nicht an ein und dieselbe Person zugewiesen werden.

HINWEIS: Nur SAP Produkte, die direkt als widersprechende Systemrollen definiert sind, können nicht an ein und dieselbe Person zugewiesen werden. Festlegungen an übergeordneten oder untergeordneten SAP Produkten haben keinen Einfluss auf die Zuweisung.

Um widersprechende Systemrollen einzusetzen

- Aktivieren Sie im Designer den Konfigurationsparameter "QER\Structures\Inherite\ESetExclusion" und kompilieren Sie die Datenbank.

Um widersprechende Systemrollen festzulegen

1. Wählen Sie die Kategorie **SAP R/3 | Produkte**.
2. Wählen Sie in der Ergebnisliste das SAP Produkt aus, für das Sie widersprechende Systemrollen definieren wollen.
3. Wählen Sie die Aufgabe **Widersprechende Systemrollen bearbeiten**.
4. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die Systemrollen, die sich mit dem gewählten SAP Produkt ausschließen.

   - ODER -

   Doppelklicken Sie im Bereich **Zuordnungen entfernen** auf die Systemrollen, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Bereitstellen der Daten für die Systemvermessung

Im One Identity Manager können die Lizenzinformationen der Benutzerkonten abgebildet werden. Eine Person kann mehrere Benutzerkonten besitzen, die unterschiedlichen Mandanten und Systemen angehören. Für die Systemvermessung wird das höchstwertige Benutzerkonto einer Person benötigt. Dieses Benutzerkonto wird durch die Systemvermessung als abzurechnendes Benutzerkonto bestimmt. Die Wertigkeit eines Benutzerkontos berechnet der One Identity Manager aus den zugeordneten Lizenzen.

Das höchstwertige Benutzerkonto einer Person wird automatisch aus allen Benutzerkonten ermittelt, die nicht über eine ZBV verwaltet werden. Für die Benutzerkonten einer ZBV werden die Lizenzinformationen im One Identity Manager abgebildet und können hier bearbeitet werden. Das höchstwertige Benutzerkonto wird jedoch nicht automatisch ermittelt.

Im One Identity Manager werden die Daten zur Systemvermessung zur Verfügung gestellt. Die eigentliche Vermessung erfolgt im Zielsystem.

Um die Daten für die Systemvermessung bereitzustellen

1. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | SAPR3 | Accounts | CalculateLicence**.
2. Aktivieren Sie am SAP System die Option **Systemvermessung aktiviert**.
3. Aktivieren Sie am Mandanten die Option **Hat Benutzerverwaltung**.
4. Erfassen Sie die Lizenzen.
    a. Erfassen Sie Lizenzen an den Rollen und Profilen. Der One Identity Manager ermittelt die Lizenz eines Benutzerkontos aus den Lizenzen aller Rollen und Profile, in denen das Benutzerkonto Mitglied ist.

    - ODER -

    b. Erfassen Sie die produktive Lizenz direkt am Benutzerkonto.

    Der One Identity Manager berechnet die höchstwertige Lizenz der Benutzerkonten aus den erfassten Lizenzen.
5. Publizieren Sie die Vermessungsdaten.

Die berechneten Lizenzen werden auf die produktiven Lizenzen übertragen. Die produktiven Lizenzen werden in das Zielsystem publiziert. Dort kann die Systemvermessung durchgeführt werden.

Detaillierte Informationen zum Thema

- SAP Systeme auf Seite 121
- Allgemeine Stammdaten eines SAP Mandanten auf Seite 122
- Lizenzen über SAP Rollen und SAP Profile ermitteln auf Seite 215
- Lizenzen an den SAP Benutzerkonten eintragen auf Seite 214
- Übertragen der berechneten Lizenzen auf Seite 217

Abbildung der Vermessungsdaten

Für Benutzerkonten, die nicht über eine ZBV verwaltet werden, werden die Vermessungsdaten auf dem Stammdatenformular der Benutzerkonten angezeigt.

Um die Vermessungsdaten anzuzeigen

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wechseln Sie auf den Tabreiter **Vermessungsdaten**.

   Das Stammdatenformular mit den synchronisierten und kalkulierten Daten zur Systemvermessung wird geöffnet.

Auf dem Formular werden die folgenden Lizenzinformationen dargestellt.

Tabelle 74: Vermessungsdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Lizenz produktiv	Lizenz des Benutzerkontos. Die produktive Lizenz wird durch die Synchronisation in die One Identity Manager-Datenbank eingelesen oder aus der kalkulierten personenbezogenen Lizenz ermittelt. HINWEIS: Die produktive Lizenz kann auch direkt bearbeitet und geändert werden. Eine Änderung der produktiven Lizenz wird sofort in das Zielsystem publiziert. Die an den Rollen und Profilen hinterlegten Lizenzen sind in diesem Fall nicht wirksam. HINWEIS: Wenn an den Rollen oder Profilen, in denen das Benutzerkonto Mitglied ist, Lizenzen hinterlegt sind und die Aufgabe **Publizieren der berechneten Lizenzen** ausgeführt wird, wird die direkt an dem Benutzerkonto hinterlegte produktive Lizenz durch die kalkulierte Lizenz überschrieben!

Eigenschaft	Beschreibung
ID Sonderversion	Lizenzerweiterung für die installierte Sonderversion. Wählen Sie aus der Auswahlliste die ID der Sonderversion. Das Eingabefeld ist nur aktiv, wenn für die produktive Lizenz Sonderversionen zugelassen sind.
Landeszuschlag	Zusätzliche Lizenzgebühr. Das Eingabefeld ist nur aktiv, wenn für die produktive Lizenz Landeszuschläge zugelassen sind.
Stellvertreter	Verweis auf das Benutzerkonto, das für einen definierten Zeitraum die Stellvertretung übernimmt. Das Eingabefeld ist aktiviert, wenn als produktive Lizenz "04 (Stellvertreter)" oder "11 (Multimandant/-system)" eingetragen ist. Das stellvertretende Benutzerkonto erhält für einen definierten Zeitraum die Rollen und Profile des angezeigten Benutzerkontos.
Stellvertretend von	Zeitraum, in dem ein anderes Benutzerkonto die Stellvertretung übernimmt. Die Eingabefelder sind aktiviert, wenn als produktive Lizenz "04 (Stellvertreter)" eingetragen ist.
Stellvertretend bis	
Lizenz kalkuliert (Mandant)	Lizenz, die aus den zugewiesenen Rollen und Profilen des Benutzerkontos innerhalb des Mandanten ermittelt wurde. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **TargetSystem | SAPR3 | Accounts | CalculateLicence**, die Option **Systemvermessung aktiviert** am SAP System und die Option **Hat Benutzerverwaltung** am SAP Mandanten aktiviert sind.
Lizenz kalkuliert (Person)	Lizenz des höchstwertigen Benutzerkontos einer Person. Für das höchstwertige Benutzerkonto ist die mandantenbezogene kalkulierte Lizenz eingetragen. Für alle anderen Benutzerkonten einer Person ist als personenbezogene kalkulierte Lizenz "11 (Multimandant/-system)" eingetragen. Diese erhalten zusätzlich einen Verweis auf das kalkulierte höchstwertige Benutzerkonto (**Ref. Name kalkuliert**). Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **TargetSystem | SAPR3 | Accounts | CalculateLicence**, die Option **Systemvermessung aktiviert** am SAP System und die Option **Hat Benutzerverwaltung** am SAP Mandanten aktiviert sind.
Ref. Name kalkuliert	Verweis auf das kalkulierte höchstwertige Benutzerkonto, wenn als kalkulierte personenbezogene Lizenz "11 (Multimandant/-system)" eingetragen ist. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **TargetSystem | SAPR3 | Accounts | CalculateLicence**, die Option **Systemvermessung aktiviert** am SAP System und die Option **Hat Benutzerverwaltung** am SAP Mandanten aktiviert sind.

Für Benutzerkonten, die über eine ZBV verwaltet werden, werden die Vermessungsdaten für jede Zuordnung eines Benutzerkontos zum Zentralsystem und zu den Tochtersystemen angezeigt.

Um die Vermessungsdaten für ein zentral verwaltetes Benutzerkonto anzuzeigen

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **SAP Lizenzen in Tochtersystem zuweisen**.
4. Wählen Sie in der Tabelle eine Zuordnung.

Auf dem Formular werden die folgenden Lizenzinformationen dargestellt.

Tabelle 75: Vermessungsdaten eines zentral verwalteten Benutzerkontos

Eigenschaft	Beschreibung
Empfängermandant	Mandant, in welchem dem Benutzerkonto eine Lizenz zugeordnet ist. Es kann das Zentralsystem oder ein zugeordnetes Tochtersystem ausgewählt werden.
Lizenz	Lizenz des Benutzerkontos im gewählten Mandanten.
Lizenzerweiterung	Lizenzerweiterung für die installierte Sonderversion. Wählen Sie aus der Auswahlliste die ID der Sonderversion.
Landeszuschlag	Zusätzliche Lizenzgebühr.
Abzurechnendes System	SAP System, in dem sich der abzurechnende Mandant befindet. Das Eingabefeld wird nur angezeigt, wenn als Lizenz "04 (Stellvertreter)" oder "11 (Multimandant/-system)" eingetragen ist.
Abzurechnender Mandant	Mandant, in dem sich das abzurechnende Benutzerkonto befindet. Das Eingabefeld wird nur angezeigt, wenn als Lizenz "04 (Stellvertreter)" oder "11 (Multimandant/-system)" eingetragen ist.
Abzurechnendes Benutzerkonto	Kostenpflichtiges Benutzerkonto, wenn als Lizenz "04 (Stellvertreter)" oder "11 (Multimandant/-system)" eingetragen ist.
Stellvertretend von	Zeitraum, in dem ein anderes Benutzerkonto die Stellvertretung übernimmt. Die Eingabefelder sind aktiviert, wenn als Lizenz "04 (Stellvertreter)" eingetragen ist.
Stellvertretend bis	

Verwandte Themen

- Lizenzen an den SAP Benutzerkonten eintragen auf Seite 214
- Lizenzen über SAP Rollen und SAP Profile ermitteln auf Seite 215
- Ermitteln der Wertigkeit eines SAP Benutzerkontos auf Seite 215
- Übertragen der berechneten Lizenzen auf Seite 217

- Sonderversionen auf Seite 105
- Lizenzen auf Seite 104

Lizenzen an den SAP Benutzerkonten eintragen

Um die Daten zur Systemvermessung direkt an den Benutzerkonten zu pflegen, erfassen Sie die produktive Lizenz an den Benutzerkonten. Das kann beispielsweise erforderlich sein, um Stellvertreterlizenzen zu hinterlegen.

Um die produktive Lizenz eines Benutzerkontos direkt zu erfassen

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie den Tabreiter **Vermessungsdaten**.
4. Wählen Sie im Eingabefeld **Lizenz produktiv** eine Lizenz aus der Auswahlliste.
5. Erfassen Sie gegebenenfalls weitere erforderliche Daten.
6. Speichern Sie die Änderungen.

   Die produktive Lizenz wird in das Zielsystem publiziert.

HINWEIS: Wenn an den Rollen oder Profilen, in denen das Benutzerkonto Mitglied ist, Lizenzen hinterlegt sind und die Aufgabe **Publizieren der berechneten Lizenzen** ausgeführt wird, wird die direkt an dem Benutzerkonto hinterlegte produktive Lizenz durch die kalkulierte Lizenz überschrieben!

Um die Lizenzen eines zentral verwalteten Benutzerkontos zu erfassen

1. Wählen Sie die Kategorie **SAP R/3 | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **SAP Lizenzen in Tochtersystem zuweisen**.
4. Klicken Sie **Hinzufügen**.

   Es wird eine neue Zeile in die Tabelle eingefügt.
5. Markieren Sie diese Zeile. Erfassen Sie die Vermessungsdaten.
6. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Abbildung der Vermessungsdaten auf Seite 211
- Lizenzen über SAP Rollen und SAP Profile ermitteln auf Seite 215

Lizenzen über SAP Rollen und SAP Profile ermitteln

Für Benutzerkonten, die nicht über eine ZBV verwaltet werden, kann die höchstwertige Lizenz aus den Lizenzen der Rollen und Profile ermittelt werden. Die Lizenzen müssen Sie nach der Synchronisation den Rollen und Profilen einmalig manuell zuordnen. Der One Identity Manager ermittelt über die Mitgliedschaften der Benutzerkonten in den Rollen und Profilen die höchstwertige Lizenz der Benutzerkonten. Das höchstwertige Benutzerkonto einer Person wird mandanten- und systemübergreifend ermittelt. Die höchstwertige Lizenz wird als produktive Lizenz an das Benutzerkonto übernommen und in das Zielsystem publiziert.

Um Lizenzen an Rollen und Profile zuzuordnen

1. Wählen Sie die Kategorie **SAP R/3 | Rollen**.

   – ODER –

   Wählen Sie die Kategorie **SAP R/3 | Profile**.
2. Wählen Sie in der Ergebnisliste die Rolle oder das Profil.
3. Ordnen Sie im Eingabegeld **Lizenz** eine Lizenz zu.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Lizenzen auf Seite 104
- Allgemeine Stammdaten von SAP Profilen auf Seite 171
- Allgemeine Stammdaten von SAP Rollen auf Seite 170

Ermitteln der Wertigkeit eines SAP Benutzerkontos

HINWEIS: Für ein leichteres Verständnis sind in diesem Abschnitt Rollen und Profile unter dem Begriff "SAP Systemberechtigungen" zusammengefasst.

Im One Identity Manager erfolgt die Ermittlung der Wertigkeit eines Benutzerkontos über die Wertigkeit der Rollen und Profile, in denen das Benutzerkonto Mitglied ist. Voraussetzung ist, dass für die Rollen und Profile die Lizenzen eingetragen wurden. Diese Zuordnung müssen Sie nach der Synchronisation dieser Objekte einmalig manuell vornehmen. Bei der Ermittlung des höchstwertigen Benutzerkontos werden die Kennung der Lizenz sowie eine eventuell manuell vergebene Lizenzwertigkeit berücksichtigt.

Zur Ermittlung der Lizenzwertigkeit wird ein Berechnungsauftrag für den DBQueue Prozessor erstellt. Der Berechnungsauftrag wird erstellt, bei

- Aktivierung des Konfigurationsparameters **TargetSystem | SAPR3 | Accounts | CalculateLicence**
- De-/Aktivierung der Option **Systemvermessung aktiviert** am SAP System
- De-/Aktivierung der Option **Hat Benutzerverwaltung** am SAP Mandanten
- Änderung der Zuweisung von Benutzerkonten zu Rollen oder Profilen
- Änderung des Gültigkeitszeitraums von Rollenzuordnungen
- Änderung der Lizenzwertigkeit einer Lizenz
- Änderung der Zuordnung von Lizenzen zu Rollen oder Profilen
- Zuordnung von Personen zu Benutzerkonten
- Änderung des Stellvertreters an einem Benutzerkonto

Das höchstwertige Benutzerkonto einer Person wird im One Identity Manager in zwei Schritten ermittelt.

1. Ermittlung der Wertigkeit des Benutzerkontos innerhalb eines Mandanten (mandantenbezogen)

   Für ein Benutzerkonto werden innerhalb eines Mandanten die Mitgliedschaften in SAP Systemberechtigungen berechnet. Daraus wird die SAP Systemberechtigung mit der höchsten Wertigkeit ermittelt. Die Lizenz der höchstwertigen SAP Systemberechtigungen wird als **Lizenz kalkuliert (Mandant)** zum Benutzerkonto übernommen. Die höchstwertige SAP Systemberechtigung erfüllt folgende Kriterien:

   a. Die zugeordnete Lizenz besitzt die niedrigste Lizenzwertigkeit (in alphanumerischer Sortierung).

   b. Wenn mehreren SAP Systemberechtigungen Lizenzen mit derselben Lizenzwertigkeit zugewiesen sind oder keine Lizenzwertigkeiten angegeben sind, gilt die Lizenz mit der höchsten Kennung.

2. Ermittlung des höchstwertigen Benutzerkontos (personenbezogen)

   a. Das höchstwertige Benutzerkonto wird über alle Benutzerkonten einer Person in allen Mandanten und allen Systemen ermittelt. Dabei gelten die unter 1 a) und 1 b) genannten Kriterien für die Benutzerkonten. Die Lizenz des höchstwertigen Benutzerkontos wird als **Lizenz kalkuliert (Person)** zum Benutzerkonto übernommen. Für alle anderen Benutzerkonten der Person wird eine Referenz auf das kalkulierte höchstwertige Benutzerkonto im Eingabefeld **Ref. Name kalkuliert** eingetragen. Diese Benutzerkonten erhalten die Lizenz "11 (Multimandant/-Systembenutzer)" oder "04 (Stellvertreter)".

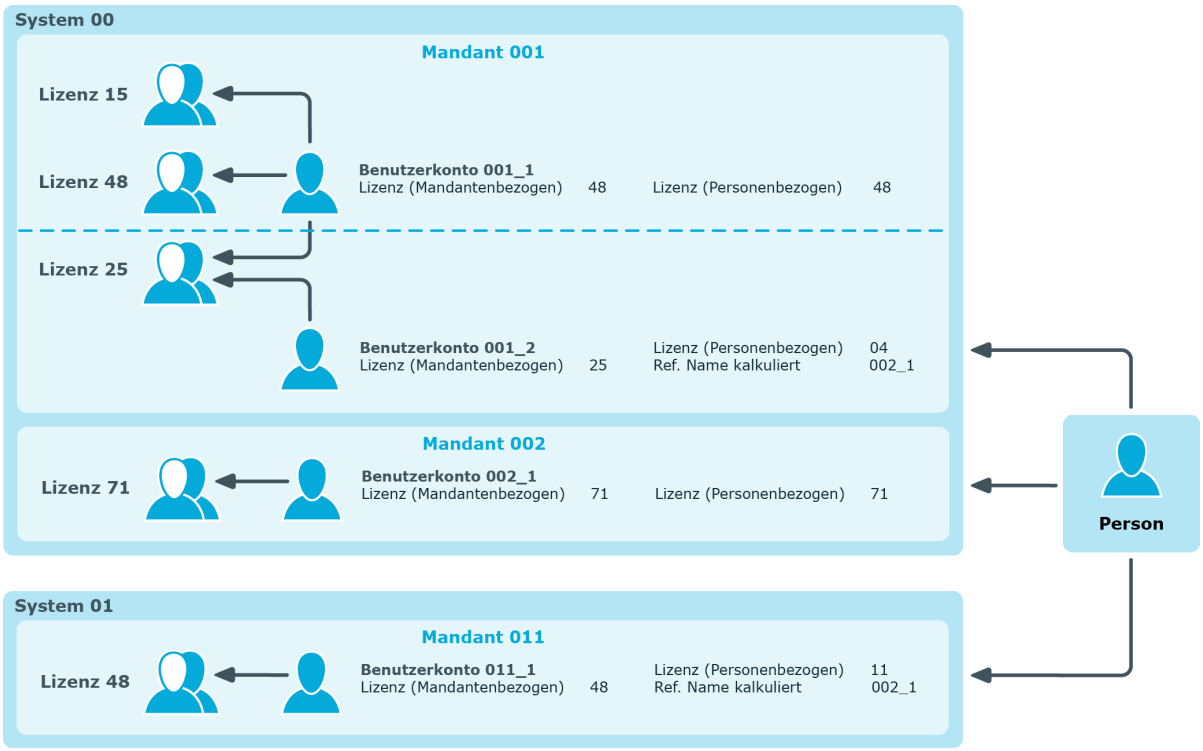
Tabelle 76: Personenbezogene Lizenz

Benutzerkonten	Lizenz kalkuliert (Person)
Höchstwertiges Benutzerkonto	Lizenz kalkuliert (Mandant)
Übrige Benutzerkonten in Mandanten des selben	04 (Stellvertreter)

Benutzerkonten	Lizenz kalkuliert (Person)
Systems wie das höchstwertige Benutzerkonto	
Übrige Benutzerkonten in anderen Systemen als das höchstwertige Benutzerkonto	11 (Multimandant/-Systembenutzer)

b. Wenn einem Benutzerkonto keine Person zugeordnet ist, dann wird die unter 1) berechnete Wertigkeit als die höchste Wertigkeit angesehen und der Lizenzeintrag als **Lizenz kalkuliert (Person)** zum Benutzerkonto übernommen.

Abbildung 6: Ermitteln der Wertigkeit eines SAP Benutzerkontos



Verwandte Themen

- Lizenzen auf Seite 104
- Lizenzberechnung deaktivieren auf Seite 219

Übertragen der berechneten Lizenzen

Damit die Vermessung in der SAP R/3-Umgebung durchgeführt werden kann, müssen Sie die personenbezogenen kalkulierten Lizenzen auf die produktiven Lizenzen übertragen.

Diese Übernahme erfolgt für jeden Mandanten eines Systems separat.

HINWEIS: Wenn die Aufgabe **Publizieren der berechneten Lizenzen** ausgeführt wird, werden manuell erfasste produktive Lizenzen an den Benutzerkonten durch die kalkulierten Lizenzen überschrieben!

Ausnahme: Als produktive Lizenz ist „04 (Stellvertreter)" eingetragen und der Zeitraum für die Stellvertretung ist aktuell gültig oder liegt in der Zukunft.

HINWEIS: Die Aufgabe **Publizieren der berechneten Lizenzen** ist nur für Mandanten mit dem ZBV Status "kein ZBV-System" oder mit leerem ZBV Status verfügbar.

Um die kalkulierten Lizenzen auf die produktiven Lizenzen zu übertragen

1. Wählen Sie die Kategorie **SAP R/3 | Mandanten**.
2. Wählen Sie in der Ergebnisliste den Mandanten, für den alle kalkulierten Lizenzen übertragen werden sollen.
3. Wählen Sie die Aufgabe **Publizieren der berechneten Lizenzen**.

   Es erscheint eine Sicherheitsabfrage.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Sobald die kalkulierten Lizenzen auf die produktiven Lizenzen übertragen wurden, werden die produktiven Lizenzen in das Zielsystem publiziert.

Der One Identity Manager überträgt für alle Benutzerkonten dieses Mandanten die kalkulierte personenbezogene Lizenz auf die produktive Lizenz. Diese Daten können Sie bei Bedarf manuell nachbearbeiten. Sobald die Lizenzen in die SAP R/3-Umgebung publiziert und die Systemvermessung durchgeführt wurden, können Sie die aktuellen Vermessungsdaten mit der One Identity Manager-Datenbank synchronisieren.

Besonderheiten für Benutzerkonten mit einer Stellvertreterlizenz

Wenn am Benutzerkonto als produktive Lizenz „04 (Stellvertreter)" eingetragen ist und der Zeitraum der Stellvertretung aktuell gültig ist, dann wird die produktive Lizenz nicht durch die kalkulierte personenbezogene Lizenz ersetzt. Gleiches gilt, wenn der Zeitraum der Stellvertretung in der Zukunft liegt (**Stellvertretend von** ist größer „heute").

Wenn der Zeitraum der Stellvertretung abgelaufen ist, wird die kalkulierte personenbezogene Lizenz durch die Aufgabe **Publizieren der berechneten Lizenzen** auf die produktive Lizenz übertragen. Die Informationen zum Stellvertreter und zum Zeitraum der Stellvertretung werden vom Benutzerkonto gelöscht.

HINWEIS: Damit eine produktive Lizenz „04 (Stellvertreter)" in die Zielsystemumgebung publiziert werden kann, müssen in der SAP R/3-Umgebung, im Programmteil Systemvermessung die Preisliste und alle verwendbaren vertraglichen Nutzertypen aktiviert sein.

Verwandte Themen

- Abbildung der Vermessungsdaten auf Seite 211
- Lizenzberechnung deaktivieren auf Seite 219

Lizenzberechnung deaktivieren

Die Ermittlung der Wertigkeit der Benutzerkonten kann für einzelne SAP Mandanten, einzelne SAP Systeme oder für alle im One Identity Manager verwalteten SAP Systeme deaktiviert werden. Die kalkulierten Lizenzen an den Benutzerkonten werden dann nicht berechnet und die produktive Lizenz nicht aktualisiert. Die an den Rollen und Profilen hinterlegten Lizenzen sind nicht wirksam. Der One Identity Manager stellt somit keine aktuellen Daten für die Systemvermessung zur Verfügung, die auf den tatsächlich zugewiesenen SAP Rollen und Profilen beruhen.

Die produktive Lizenz kann weiterhin direkt erfasst und in das Zielsystem publiziert werden. Werden produktive Lizenzen in der Zielsystemumgebung geändert, werden diese Änderungen durch die Synchronisation in die One Identity Manager-Datenbank eingelesen.

Um die Lizenzberechnung zu deaktivieren

- Deaktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | SAPR3 | Accounts | CalculateLicence**.

  - ODER -

- Deaktivieren Sie am SAP System die Option **Systemvermessung aktiviert**.

  - ODER -

- Deaktivieren Sie am Mandanten die Option **Hat Benutzerverwaltung**.

Verwandte Themen

- Ermitteln der Wertigkeit eines SAP Benutzerkontos auf Seite 215
- Übertragen der berechneten Lizenzen auf Seite 217

11

Berichte über SAP Systeme

Der One Identity Manager stellt verschiedene Berichte zur Verfügung, in denen Informationen über das ausgewählte Basisobjekt und seine Beziehungen zu anderen Objekten der One Identity Manager-Datenbank aufbereitet sind. Für SAP Systeme stehen folgende Berichte zur Verfügung.

HINWEIS: Abhängig von den vorhandenen Modulen können weitere Berichte zur Verfügung stehen.

Tabelle 77: Berichte für das Zielsystem

Bericht	Beschreibung
Übersicht aller Zuweisungen (System)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten System mindestens ein Benutzerkonto besitzen.
Übersicht aller Zuweisungen (Mandant)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Mandanten mindestens ein Benutzerkonto besitzen.
Übersicht aller Zuweisungen (Gruppe, Rolle, Profil)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, welche die ausgewählte Gruppe, Rolle oder das Profil besitzen.
Unverbundene Benutzerkonten anzeigen	Der Bericht zeigt alle Benutzerkonten des Mandanten, denen keine Person zugeordnet ist. Der Bericht enthält die zugeordneten Systemberechtigungen und die Risikoeinschätzung.
Personen mit mehreren Benutzerkonten anzeigen	Der Bericht zeigt alle Personen, die mehrere Benutzerkonten in dem Mandanten besitzen. Der Bericht enthält eine Risikoeinschätzung.
Abweichende Systemberechtigungen anzeigen	Der Bericht enthält alle Systemberechtigungen des Mandanten, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager.
Ungenutzte Benutzerkonten anzeigen	Der Bericht enthält alle Benutzerkonten des Mandanten, die in den letzten Monaten nicht genutzt wurden.

Bericht	Beschreibung
Benutzerkonten mit einer überdurchschnittlichen Anzahl an System-berechtigungen anzeigen	Der Bericht enthält alle Benutzerkonten des Mandanten, die eine überdurchschnittliche Anzahl an Systemberechtigungen besitzen.
SAP Benutzerkonten- und Gruppenverteilung	Der Bericht enthält eine Zusammenfassung der Benut-zerkonten- und Gruppenverteilung aller Mandanten. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager | Übersichten Zielsysteme**.
Datenqualität der SAP Benutzerkonten	Der Bericht enthält verschiedenen Auswertungen zur Daten-qualität der Benutzerkonten aller Mandanten. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager | Analyse Datenqualität**.

Übersicht aller Zuweisungen

Für einige Objekte, wie beispielsweise Berechtigungen, Complianceregeln oder Rollen wird der Bericht **Übersicht aller Zuweisungen** angezeigt. Der Bericht ermittelt alle Rollen, wie beispielsweise Abteilungen, Kostenstellen, Standorte, Geschäftsrollen und IT Shop Strukturen, in denen sich Personen befinden, die das gewählte Basisobjekt besitzen. Dabei werden sowohl direkte als auch indirekte Zuweisungen des Basisobjektes berücksichtigt.

Beispiele

- Wird der Bericht für eine Ressource erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Ressource besitzen.
- Wird der Bericht für eine Gruppe oder andere Systemberechtigung erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Gruppe oder Systemberechtigung besitzen.
- Wird der Bericht für eine Complianceregel erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Complianceregel verletzen.
- Wird der Bericht für eine Abteilung erstellt, werden alle Rollen ermittelt, in denen die Personen der gewählten Abteilung ebenfalls Mitglied sind.
- Wird der Bericht für eine Geschäftsrolle erstellt, werden alle Rollen ermittelt, in denen die Personen der gewählten Geschäftsrolle ebenfalls Mitglied sind.

Um detaillierte Informationen über Zuweisungen anzuzeigen

- Um den Bericht anzuzeigen, wählen Sie in der Navigation oder in der Ergebnisliste das Basisobjekt und wählen Sie den Bericht **Übersicht aller Zuweisungen**.
- Wählen Sie über die Schaltfläche **Verwendet von** in der Symbolleiste des Berichtes die Rollenklasse, für die Sie ermitteln möchten, ob es Rollen gibt, in denen

sich Personen mit dem ausgewählten Basisobjekt befinden.

Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Personen befinden, denen das ausgewählte Basisobjekt zugewiesen ist. Die Bedeutung der Steuerelemente des Berichts ist in einer separaten Legende erläutert. Die Legende erreichen Sie über das Symbol in der Symbolleiste des Berichtes.

- Mit einem Maus-Doppelklick auf das Steuerelement einer Rolle zeigen Sie alle untergeordneten Rollen der ausgewählten Rolle an.
- Mit einem einfachen Mausklick auf die Schaltfläche im Steuerelement einer Rolle zeigen Sie alle Personen dieser Rolle an, die das Basisobjekt besitzen.
- Über den Pfeil rechts neben der Schaltfläche starten Sie einen Assistenten, mit dem Sie die Liste der angezeigten Personen zur Nachverfolgung speichern können. Dabei wird eine neue Geschäftsrolle erstellt und die Personen werden der Geschäftsrolle zugeordnet.

Abbildung 7: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 78: Bedeutung der Symbole in der Symbolleiste des Berichts

Symbol	Bedeutung
	Anzeigen der Legende mit der Bedeutung der Steuerelemente des Berichts.
	Speichern der aktuellen Ansicht des Berichts als Bild.
	Auswählen der Rollenklasse, über die der Bericht erstellt werden soll.
	Anzeige aller Rollen oder Anzeige der betroffenen Rolle.

Anhang A

Konfigurationsparameter für die Verwaltung einer SAP R/3-Umgebung

Mit der Installation des Moduls sind zusätzlich folgende Konfigurationsparameter im One Identity Manager verfügbar.

Tabelle 79: Konfigurationsparameter

Konfigurationsparameter	Beschreibung
TargetSystem | SAPR3	Der Bereich SAP wird unterstützt. Der Parameter ist ein präprozessorrelevanter Konfigurationsparameter. Die Aktivierung oder Deaktivierung erfordert eine Kompilierung der Datenbank.
TargetSystem | SAPR3 | Accounts	Standardwerte für SAP Benutzerkonten sollen verwendet werden.
TargetSystem | SAPR3 | Accounts | CalculateLicence	Parameter zur Steuerung der Berechnung der SAP Systemvermessung für SAP Benutzerkonten.
TargetSystem | SAPR3 | Accounts | Datfm	Festlegung des Standard-Datumsformates für SAP Benutzerkonten.
TargetSystem | SAPR3 | Accounts | Dcpfm	Festlegung des Standard-Dezimalpunktformates für SAP Benutzerkonten.
TargetSystem | SAPR3 | Accounts | ExtID_Type	Festlegung des Standardtyps für externe Kennungen für SAP Benutzerkonten.
TargetSystem | SAPR3 | Accounts | Fax_Group	Festlegung der Standard-Faxgruppe für SAP Benutzerkonten.
TargetSystem | SAPR3 | Accounts | Guiflag	Festlegung für SAP Benutzerkonten, ob die unsichere Kommunikation erlaubt ist.
TargetSystem | SAPR3 | Accounts |	Der Konfigurationsparameter legt fest, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes

Konfigurationsparameter	Beschreibung
InitialRandomPassword	Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in der zugewiesenen Kennwortrichtlinie definiert sind.
TargetSystem | SAPR3 | Accounts | InitialRandomPassword | SendTo	Der Konfigurationsparameter enthält die Person, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Geschäftsrolle, Verantwortlicher der Person oder `XUserInserted`). Ist kein Empfänger ermittelbar, dann wird an die im Konfigurationsparameter "TargetSystem | SAPR3 | DefaultAddress" hinterlegte Adresse versandt.
TargetSystem | SAPR3 | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den Anmeldeinformationen zum Benutzerkonto zu versorgen. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto** verwendet.
TargetSystem | SAPR3 | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den Informationen zum initialen Kennwort zu versorgen. Es wird die Mailvorlage **Person - Initiales Kennwort für neues Benutzerkonto** verwendet.
TargetSystem | SAPR3 | Accounts | Langu_p	Festlegung des Standard-Sprachenschlüssels für SAP Benutzerkonten.
TargetSystem | SAPR3 | Accounts | Langup_iso	Festlegung der Standardsprache (ISO 639).
TargetSystem | SAPR3 | Accounts | MailTemplateDefaultValues	Der Konfigurationsparameter enthält die Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto mit Standardwerten** verwendet.
TargetSystem | SAPR3 | Accounts | Spda	Festlegung der Standardeinstellung für Druckparameter 3 (Löschen nach Druck).
TargetSystem | SAPR3 | Accounts | Spdb	Festlegung der Standardeinstellung für Druckparameter 2 (Drucken sofort).
TargetSystem | SAPR3 | Accounts | Splg	Festlegung des Standarddruckers (Druckparameter 1).
TargetSystem | SAPR3 | Accounts | TargetSystemID	Festlegung der Standard-Zielsystemkennung für die Abbildung externer Benutzer

Konfigurationsparameter	Beschreibung
TargetSystem | SAPR3 | Accounts | Time_zone	Festlegung des Standardwertes für die Zeitzone der Adresse eines SAP Benutzerkontos.
TargetSystem | SAPR3 | Accounts | Tzone	Festlegung des Standardwertes für die Zeitzone.
TargetSystem | SAPR3 | Accounts | Ustyp	Festlegung des Standard-Benutzertyps für SAP Benutzerkonten.
TargetSystem | SAPR3 | AutoCreateDepartment	Der Konfigurationsparameter legt fest, ob beim Synchronisieren oder Ändern von Benutzerkonten automatisch Abteilungen erzeugt werden.
TargetSystem | SAPR3 | DefaultAddress	Standard-E-Mail-Adresse (Empfänger) für Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem | SAPR3 | KeepRedundantProfiles	Der Konfigurationsparameter regelt das Verhalten für die Behandlung von Einzelrollen- und Profilzuweisungen an Benutzer. Ist der Parameter aktiviert, bleiben Einzelrollen oder Profile des Benutzers, die bereits Bestandteil von Sammelrollen des Benutzers sind, erhalten. Ist der Parameter deaktiviert, werden Einzelrollen oder Profile des Benutzers, die bereits Bestandteil von Sammelrollen des Benutzers sind, entfernt (Standard).
TargetSystem | SAPR3 | MaxFullsyncDuration	Angabe der maximalen Laufzeit für eine Synchronisation.
TargetSystem | SAPR3 | PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem | SAPR3 | PersonAutoDisabledAccounts	Der Konfigurationsparameter legt fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem | SAPR3 | PersonAutoFullsync	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem | SAPR3 | ValidDateHandling	Konfigurationsparameter zur Behandlung der Gültigkeitsdaten in Zuweisungen von SAP Rollen und strukturellen Profilen an SAP Benutzerkonten.
TargetSystem | SAPR3 |	Der Konfigurationsparameter legt fest, ob die Gültig-

Konfigurationsparameter	Beschreibung
ValidDateHandling | DoNotUsePWODate	keitsdaten aus dem Bestellvorgang in die Zuweisung von SAP Rollen und strukturellen Profilen an SAP Benutzerkonten übernommen werden. Wenn der Konfigurationsparameter aktiviert ist, werden die Daten **Gültig von** und **Gültig bis** nicht aus dem Bestellvorgang an die Zuweisungen übernommen.
TargetSystem | SAPR3 | ValidDateHandling | ReuseInheritedDate	Steuert die Nachnutzung bereits vorhandener Zuweisungen von SAP Rollen und strukturellen Profilen an SAP Benutzerkonten. Wenn der Konfigurationsparameter aktiviert ist, werden bereits vorhandene Zuweisungen nachgenutzt, wenn dieselbe Zuweisung über verschiedene Vererbungswege entsteht und der Gültigkeitszeitraum übereinstimmt.
TargetSystem | SAPR3 | ValidDateHandling | ReuseInheritedDate | UseTodayForInheritedValidFrom	Der Konfigurationsparameter legt fest, ob das **Gültig von**-Datum indirekter Zuweisungen von SAP Rollen und strukturellen Profilen an SAP Benutzkonten auf **<Heute>** oder auf **1900-01-01** gesetzt wird.
TargetSystem | SAPR3 | VerifyUpdates	Der Konfigurationsparameter legt fest, ob bei einem Update geänderte Eigenschaften im Zielsystem überprüft werden. Ist der Parameter aktiviert, werden nach jedem Update die Eigenschaften des Objektes im Zielsystem verifiziert.

Anhang B

Standardprojektvorlagen für die Synchronisation einer SAP R/3-Umgebung

Eine Standardprojektvorlage sorgt dafür, dass alle benötigten Informationen im One Identity Manager angelegt werden. Dazu gehören beispielsweise die Mappings, Workflows und das Basisobjekt der Synchronisation. Wenn Sie keine Standardprojektvorlage verwenden, müssen Sie das Basisobjekt der Synchronisation selbst im One Identity Manager bekannt geben.

Verwenden Sie eine Standardprojektvorlage für die initiale Einrichtung des Synchronisationsprojektes. Für kundenspezifische Implementierungen können Sie das Synchronisationsprojekt mit dem Synchronization Editor erweitern.

Detaillierte Informationen zum Thema

- Projektvorlage für Mandanten ohne ZBV auf Seite 227
- Projektvorlage für das Zentralsystem einer ZBV auf Seite 229
- Projektvorlage für untergeordnete ZBV-Systeme auf Seite 230

Projektvorlage für Mandanten ohne ZBV

Für die Synchronisation von Mandanten, die nicht an eine Zentrale Benutzerverwaltung angeschlossen sind, nutzen Sie die Projektvorlage "SAP® R/3® Synchronisation (Basisadministration)". Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 80: Abbildung der SAP R/3-Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im Zielsystem	Tabelle im One Identity Manager Schema
Company	SAPCompany

Schematyp im Zielsystem	Tabelle im One Identity Manager Schema
GROUP	SAPGrp
LICENSETYPE	SAPLicence
LicenceExtension	SAPLicenceExtension
LoginLanguage	SAPLoginLanguages
MANDANT	SAPMandant
Parameter	SAPParameter
Printer	SAPPrinter
PROFILE	SAPProfile
ProfileInProfile	SAPProfileInSAPProfile
ProfileInRole	SAPProfileInSAPRole
PROFITCENTER	SAPProfitCenter
ROLE	SAPRole
RoleInRole	SAPRoleInSAPRole
STARTMENUE	SAPStartMenu
SAPTSAD3T	SAPTitle
USER	SAPUser
UserComFax	SAPComFax
UserComPhone	SAPComPhone
UserComSMTP	SAPComSMTP
SAPCOMMTYPE	SAPCommType
UserExtId	SAPUserExtId
UserHasParameter	SAPUserHasParameter
UserInGroup	SAPUserInSAPGrp
UserInProfile	SAPUserInSAPProfile
UserInRole	SAPUserInSAPRole

Projektvorlage für das Zentralsystem einer ZBV

Für die Synchronisation des Zentralsystems einer Zentrale Benutzerverwaltung, nutzen Sie die Projektvorlage "SAP® R/3® Synchronisation (Basisadministration)". Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 81: Abbildung der SAP R/3-Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im Zielsystem	Tabelle im One Identity Manager Schema
ALE	SAPMandant
MANDANT	SAPMandant
Company	SAPCompany
GROUP	SAPGrp
LICENSETYPE	SAPLicence
LicenceExtension	SAPLicenceExtension
LoginLanguage	SAPLoginLanguages
Parameter	SAPParameter
Printer	SAPPrinter
CUAProfile	SAPProfile
ProfileInProfile	SAPProfileInSAPProfile
ProfileInRole	SAPProfileInSAPRole
PROFITCENTER	SAPProfitCenter
CUARole	SAPRole
RoleInRole	SAPRoleInSAPRole
STARTMENUE	SAPStartMenu
SAPTSAD3T	SAPTitle
USER	SAPUser
UserComFax	SAPComFax
UserComPhone	SAPComPhone
UserComSMTP	SAPComSMTP
UserExtId	SAPUserExtId

Schematyp im Zielsystem	Tabelle im One Identity Manager Schema
UserHasLicense	SAPUserHasLicence
UserHasParameter	SAPUserHasParameter
UserInGroup	SAPUserInSAPGrp
UserInMandant	SAPUserInSAPMandant
UserInCUAProfile	SAPUserInSAPProfile
UserInCUARole	SAPUserInSAPRole

Projektvorlage für untergeordnete ZBV-Systeme

Für die Synchronisation von Tochtersystemen einer Zentrale Benutzerverwaltung, die sich nicht im selben SAP System befinden, wie das Zentralsystem, nutzen Sie die Projektvorlage "SAP® R/3® (untergeordnetes ZBV System)". Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 82: Abbildung der SAP R/3-Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im Zielsystem	Tabelle im One Identity Manager Schema
LICENSETYPE	SAPLicence
LicenceExtension	SAPLicenceExtension
LoginLanguage	SAPLoginLanguages
MANDANT	SAPMandant

Anhang C

Referenzierte SAP R/3-Tabellen und BAPI-Aufrufe

Folgende Übersicht gibt Auskunft über alle während einer Synchronisation referenzierten Tabellen in einer SAP R/3-Umgebung und die ausgeführten BAPI-Aufrufe.

Tabelle 83: Referenzierte Tabellen und BAPIs

Tabellen	BAPI-Aufrufe
• ADR2 • ADR3 • ADR6 • AGR_1016 • AGR_AGRS • AGR_DEFINE • AGR_USERS • ANLA • ANLZ • CSKS • CSKT • DD02L • DD03L • DD04L • DD07L • RSECUSERAUTH • RSECTXT • SEC_POLICY_CUST • SEC_POLICY_RT	• BAPI_USER_CREATE1 • BAPI_USER_GET_DETAIL • BAPI_USER_CHANGE • BAPI_USER_DELETE • BAPI_USER_LOCK • BAPI_USER_UNLOCK • BAPI_USER_ACTGROUPS_ASSIGN • BAPI_USER_ACTGROUPS_DELETE • BAPI_USER_PROFILES_ASSIGN • BAPI_USER_PROFILES_DELETE • BAPI_USER_LOCACTGROUPS_READ • BAPI_USER_LOCACTGROUPS_DELETE • BAPI_USER_LOCPROFILES_READ • BAPI_USER_LOCPROFILES_DELETE • BAPI_USER_SYSTEM_ASSIGN • SUSR_USER_CHANGE_PASSWORD_RFC • BAPI_USER_LOCPROFILES_ASSIGN • BAPI_USER_LOCACTGROUPS_ASSIGN • RFC_READ_TABLE

Tabellen	BAPI-Aufrufe
• T000 • T001 • T002 • T591S • T500P • T548T • TMENU01 • TMENU01R • TPARA • TSAD3 • TSAD3T • TSAC • TSADC • TSP03 • TTREE • TUTYPA • TUTYPPL • TUZUS • USGRP_USER • USL04 • USLA04 • USR01 • USR02 • USR05 • USR06 • USR06SYS • USR12 • USR21 • USREFUS • USREXTID • UST04 • UST10C • USZBVLNDSC	

Tabellen	BAPI-Aufrufe
• USZBVLNDRC • USZBVSYS • USRSYSACTT • USRSYSPRF • USRSTAMP • V_USCOMPA	

Anhang D

Beispiel für eine Schemaerweiterungsdatei

```
<?xml version="1.0" encoding="utf-8" ?>
<SAP>
     <Functions>
          <Function Definition = "USER GET" FunctionName="BAPI_USER_GET_DETAIL"
          OutStructure = "" Key ="USERNAME" X500 ="CN">
               <Mapping>
                    <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
               </Mapping>
          </Function>
          <Function Definition = "USER SET" FunctionName="BAPI_USER_CHANGE"
          OutStructure ="" Key ="USERNAME" X500 ="CN">
               <Mapping>
                    <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
               </Mapping>
          </Function>
          <Function Definition = "USER DEL" FunctionName="BAPI_USER_DELETE"
          OutStructure ="" Key ="USERNAME" X500 ="CN">
               <Mapping>
                    <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
               </Mapping>
          </Function>
          <Function Definition = "USER PROFILE SET" FunctionName="BAPI_USER_PROFILES_
          ASSIGN" OutStructure ="" Key ="USERNAME" X500 ="CN">
               <Mapping>
                    <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
```

```
            <Data ParameterName = "BAPIPROF~BAPIPROF" PropertyName =
            "$Value$" />
        </Mapping>
    </Function>
    <Function Definition = "BWProfileAdd" FunctionName="/VIAENET/SAPHR_
    RSECUSERAUT_ADD" OutStructure ="" Key ="ZUSRNAME,ZHIER" X500 ="CN,OU">
        <Mapping>
            <Data ParameterName = "ZUSRNAME" PropertyName = "UNAME" />
            <Data ParameterName = "ZHIER" PropertyName = "AUTH" />
        </Mapping>
    </Function>
    <Function Definition = "BWProfileDel" FunctionName="/VIAENET/SAPHR_
    RSECUSERAUT_DEL" OutStructure ="" Key ="ZUSRNAME,ZHIER" X500 ="CN,OU">
        <Mapping>
            <Data ParameterName = "ZUSRNAME" PropertyName = "UNAME" />
            <Data ParameterName = "ZHIER" PropertyName = "AUTH" />
        </Mapping>
    </Function>
    <Function Definition = "BWProfileDelFkt" FunctionName="/VIAENET/SAPHR_
    RSECUSERAUT_DEL" OutStructure ="" Key ="ZUSRNAME,ZHIER" X500 ="CN,OU">
        <Mapping>
            <Data ParameterName = "ZUSRNAME" PropertyName = "BNAME" />
            <Data ParameterName = "ZHIER" PropertyName = "$VALUE$" />
        </Mapping>
    </Function>
    <Function Definition = "BWProfileAddFkt" FunctionName="/VIAENET/SAPHR_
    RSECUSERAUT_ADD" OutStructure ="" Key ="ZUSRNAME,ZHIER" X500 ="CN,OU">
        <Mapping>
            <Data ParameterName = "ZUSRNAME" PropertyName = "BNAME" />
            <Data ParameterName = "ZHIER" PropertyName = "$VALUE$" />
        </Mapping>
    </Function>
</Functions>
<Tables>
    <TABLE Definition = "TUZUS-Table" TableName="TUZUS" Key="SONDERVERS"
    X500="CN" SQL="LANGU = sy-langu" Load="SONDERVERS,TEXTSVERS" />
```

```
        <TABLE Definition = "USR05-Tabelle" TableName="USR05" Key="BNAME,PARID"
        X500="CN,OU" SQL="MANDT = '$MANDT$'" Load="BNAME,PARID,PARVA">
            <Mapping>
                <Data ParameterName = "$BNAME$" PropertyName = "BNAME" />
                <Data ParameterName = "$PARID$" PropertyName = "PARID" />
            </Mapping>
        </TABLE>
        <TABLE Definition = "USR04-Tabelle" TableName="USR04" Key="BNAME,MANDT"
        X500="CN,OU" SQL="MANDT = sy-mandt" Load="" />
        <TABLE Definition = "RSECUSERAUTH-Table" TableName="RSECUSERAUTH"
        Key="UNAME,AUTH" X500="CN,OU" SQL="" Load="" />
        <TABLE Definition = "RSECUSERAUTH-SingleUser" TableName="RSECUSERAUTH"
        Key="AUTH" X500="CN" SQL="UNAME = '$BNAME$'" Load="">
            <Mapping>
                <Data ParameterName = "$BNAME$" PropertyName = "BNAME" />
            </Mapping>
        </TABLE>
    </Tables>
    <SAPExtendedSchematypes>
        <SAPExtendedSchematype Bem = "M:N, add/del - funktion" Name = "BWUserInBWP"
        DisplayPattern="%UNAME% - %AUTH%" ListObjectsDefinition = "RSECUSERAUTH-
        Table" ReadObjectDefinition = "RSECUSERAUTH-Table" InsertObjectDefinition =
        "BWProfileAdd" DeleteObjectDefinition = "BWProfileDel" />
        <SAPExtendedSchematype Bem = "simple read only table" Name =
        "LicenceExtension" DisplayPattern="%SONDERVERS%" ListObjectsDefinition =
        "TUZUS-Table" ReadObjectDefinition ="TUZUS-Table" InsertObjectDefinition =
        "" WriteObjectDefinition = "" DeleteObjectDefinition = "" ParentType =
        "SAPSYSTEM" />
        <SAPExtendedSchematype Bem = "Test" Name = "USERFunctionTable"
        DisplayPattern="%BNAME% (%MANDT%)" ListObjectsDefinition = "USR05-Tabelle"
        ReadObjectDefinition ="USER GET" WriteObjectDefinition = "USER SET"
        DeleteObjectDefinition = "USER DEL" >
            <Properties>
                <Property Name = "SAPBWP" Description="alle BW Profile des
                Users" ListFunction="RSECUSERAUTH-SingleUser"
                AddFunction="BWProfileAddFkt" DelFunction="BWProfileDelFkt"
                ReplaceFunction="" IsMultivalued = "true" />
                <Property Name = "USERPROFILE" Description="alle Profile des
                Users" ListFunction="USR04-Tabelle" AddFunction=""
```

```
                    DelFunction="" ReplaceFunction="USER PROFILE SET" IsMultivalued
                    = "true" />
                </Properties>
            </SAPExtendedSchematype>
        </SAPExtendedSchematypes>
</SAP>
```

Über uns

One Identity Lösungen eliminieren die Komplexität und die zeitaufwendigen Prozesse, die häufig bei der Identity Governance, der Verwaltung privilegierter Konten und dem Zugriffsmanagement aufkommen. Unsere Lösungen fördern die Geschäftsagilität und bieten durch lokale, hybride und Cloud-Umgebungen eine Möglichkeit zur Bewältigung Ihrer Herausforderungen beim Identitäts- und Zugriffsmanagement.

Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen, wie Lizenzierungen, Support oder Support-Erneuerungen, besuchen Sie https://www.oneidentity.com/company/contact-us.aspx.

Technische Supportressourcen

Technische Unterstützung steht für One Identity Kunden mit einem gültigen Wartungsvertrag und Kunden mit Testversionen zur Verfügung. Sie können auf das Support Portal unter https://support.oneidentity.com/ zugreifen.

Das Support Portal bietet Selbsthilfe-Tools, die Sie verwenden können, um Probleme schnell und unabhängig zu lösen, 24 Stunden am Tag, 365 Tage im Jahr. Das Support Portal ermöglicht Ihnen:

- Senden und Verwalten von Serviceanfragen
- Anzeigen von Knowledge Base Artikeln
- Anmeldung für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Videos unter www.YouTube.com/OneIdentity
- Engagement in der One Identity Community
- Chat mit Support-Ingenieuren
- Anzeigen von Diensten, die Sie bei Ihrem Produkt unterstützen

Index

D

E

F

G

I

J

K

L

M

O

P

R

S

T

V

Z