One Identity Manager 8.1.5

Administrationshandbuch für die Anbindung einer Oracle E-Business Suite

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 Oracle E-Business Suite
Aktualisiert - 09. Juli 2021, 12:33 Uhr
Version - 8.1.5

Inhalt

Abbilden einer Oracle E-Business Suite im One Identity Manager

Der One Identity Manager bietet eine vereinfachte Administration der Benutzer einer Oracle E-Business Suite. Dabei konzentriert sich der One Identity Manager auf die Einrichtung und Bearbeitung von Benutzerkonten sowie die Versorgung mit den benötigten Berechtigungen. Dafür werden Applikationen, Zuständigkeiten, Datengruppen und Datengruppeneinheiten, Sicherheitsgruppen, Prozessgruppen, Menüs und Attribute im One Identity Manager abgebildet.

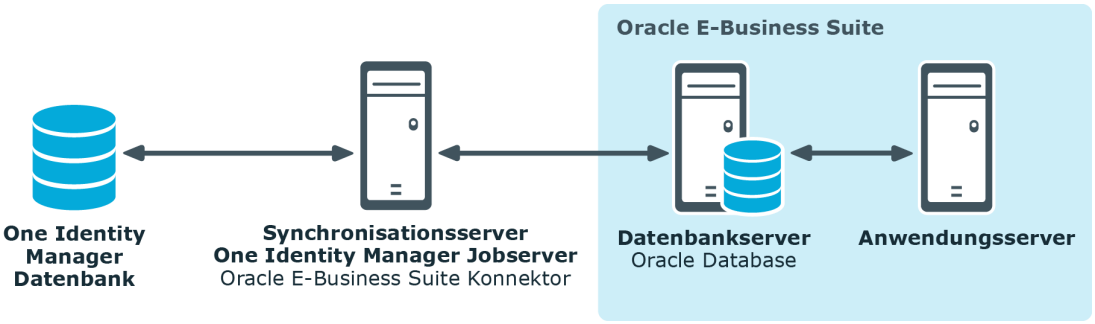
Im One Identity Manager werden die Personen eines Unternehmens mit den benötigten Benutzerkonten versorgt. Dabei können Sie unterschiedliche Mechanismen für die Verbindung der Personen mit ihren Benutzerkonten nutzen. Ebenso können Sie die Benutzerkonten getrennt von Personen verwalten und somit administrative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

Zusätzlich können Daten aus dem Human Resources Modul (Personendaten und Standorte) und organisatorische Daten (Lieferanten, Kunden, andere Beteiligte) importiert werden. Die importierten Personen können über ihre E-Business Suite Benutzerkonten mit allen erforderlichen Berechtigungen in der E-Business Suite versorgt werden. Die Standardfunktionen des One Identity Manager, wie IT Shop oder Identity Audit, können für diese Personen genutzt werden.

Architekturüberblick

Um auf die Daten einer Oracle E-Business Suite zuzugreifen, wird auf einem Synchronisationsserver der Oracle E-Business Suite Konnektor installiert. Der Oracle E-Business Suite Konnektor stellt die Kommunikation mit der zu synchronisierenden Oracle E-Business Suite her. Der Synchronisationsserver sorgt für den Abgleich der Daten zwischen der One Identity Manager-Datenbank und der Oracle Database.

Abbildung 1: Architektur für die Synchronisation



One Identity Manager Benutzer für die Verwaltung einer Oracle E-Business Suite

In die Einrichtung und Verwaltung einer E-Business Suite 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 | Oracle E-Business Suite** oder einer untergeordneten Anwendungsrolle

Benutzer	Aufgaben
	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 Berechtigungen 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. • 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.

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 Oracle E-Business Suite auf Seite 172.

2

Synchronisieren einer Oracle E-Business Suite

Der One Identity Manager unterstützt die Synchronisation mit den Oracle E-Business Suite Versionen 12.1 und 12.2. Für den Abgleich der Informationen zwischen der One Identity Manager-Datenbank und der Oracle E-Business Suite sorgt der One Identity Manager Service.

Informieren Sie sich hier:

- wie Sie die Synchronisation einrichten, um initial Daten aus einer Oracle E-Business Suite in die One Identity Manager-Datenbank einzulesen,
- wie Sie eine Synchronisationskonfiguration anpassen, beispielsweise um verschiedene E-Business Suite Systeme mit ein und demselben Synchronisationsprojekt zu synchronisieren,
- wie Sie die Synchronisation starten und deaktivieren,
- wie Sie die Synchronisationsergebnisse auswerten.

TIPP: Bevor Sie die Synchronisation mit einer Oracle E-Business Suite einrichten, machen Sie sich mit dem Synchronization Editor vertraut. Ausführliche Informationen über dieses Werkzeug finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Detaillierte Informationen zum Thema

- Einrichten der Initialsynchronisation auf Seite 13
- Anpassen einer Synchronisationskonfiguration auf Seite 29
- Ausführen einer Synchronisation auf Seite 49
- Fehleranalyse auf Seite 55
- Verarbeitung von Systemobjekten auf Seite 170

Verwandte Themen

- Architekturüberblick auf Seite 8

Einrichten der Initialsynchronisation

Der Synchronization Editor stellt verschiedene Projektvorlagen bereit, mit denen wahlweise die Synchronisation von Benutzerkonten und Berechtigungen der Oracle E-Business Suite, von organisatorischen Daten oder von Daten aus dem Human Resources Modul eingerichtet werden kann. Nutzen Sie diese Projektvorlagen, um Synchronisationsprojekte zu erstellen, mit denen Sie Daten aus einer Oracle E-Business Suite in Ihre One Identity Manager-Datenbank einlesen. Zusätzlich werden die notwendigen Prozesse angelegt, über die Änderungen an Zielsystemobjekten aus der One Identity Manager-Datenbank in das Zielsystem provisioniert werden.

Um eine Synchronisationskonfiguration für die initiale Synchronisation einer Oracle E-Business Suite zu erstellen

1. Stellen Sie in der Oracle E-Business Suite ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Die One Identity Manager Bestandteile für die Verwaltung von Oracle E-Business Suite-Umgebungen sind verfügbar, wenn der Konfigurationsparameter **TargetSystem | EBS** 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.
3. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
4. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Detaillierte Informationen zum Thema

- Benutzer und Berechtigungen für die Synchronisation mit einer Oracle E-Business Suite auf Seite 14
- Systemanforderungen für den Synchronisationsserver auf Seite 17
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Oracle E-Business Suite auf Seite 20
- Konfigurationsparameter für die Verwaltung einer Oracle E-Business Suite auf Seite 172
- Standardprojektvorlagen für die Synchronisation einer Oracle E-Business Suite auf Seite 167

Benutzer und Berechtigungen für die Synchronisation mit einer Oracle E-Business Suite

Bei der Synchronisation des One Identity Manager mit einer Oracle E-Business Suite spielen folgende Benutzer eine Rolle.

Tabelle 2: Benutzer für die Synchronisation

Benutzer	Berechtigungen
Benutzer für den Zugriff auf das Zielsystem (Synchronisationsbenutzer)	Für eine vollständige Synchronisation von Objekten einer Oracle E-Business Suite mit der ausgelieferten One Identity Manager Standardkonfiguration stellen Sie ein Benutzerkonto bereit, das die benötigten Mindestberechtigungen besitzt. Weitere Informationen finden Sie unter Bereitstellen eines Synchronisationsbenutzers auf Seite 15 und Benötigte Berechtigungen für die Synchronisation mit einer Oracle E-Business Suite auf Seite 164.
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"` 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 Betriebs-

Benutzer	Berechtigungen
	systemen) • `%ProgramFiles%\One Identity` (auf 64-Bit Betriebs-systemen)
Benutzer für den Zugriff auf die One Identity Manager-Datenbank	Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer **Synchronization** bereitgestellt.

Bereitstellen eines Synchronisationsbenutzers

Um einen Benutzer mit allen erforderlichen Berechtigungen für den Zugriff auf die Oracle E-Business Suite bereitzustellen, nutzen Sie eine der folgenden drei Möglichkeiten:

Szenario 1:	Nutzen Sie den Benutzer **APPS** als Synchronisationsbenutzer.
Szenario 2:	Spielen Sie das mitgelieferte Wrapper-Package in das APPS-Schema ein und legen Sie den Synchronisationsbenutzer über das mitgelieferte Skript an.
Szenario 3:	Legen Sie einen Synchronisationsbenutzer an, der alle aufgelisteten Minimalberechtigungen besitzt.

In der Oracle E-Business Suite Version 12.2 wurden die Aufrufrechte der Standard-Packages geändert (`CURRENT_USER AUTHID` anstelle von `DEFINER AUTHID`). Um Operationen für Benutzerkonten im Zielsystem ausführen zu können, wird nun der Benutzer **APPS** benötigt. Nutzen Sie in diesem Fall Szenario 1 oder 2, um den Synchronisationsbenutzer bereitzustellen. Wenn Sie mit Oracle E-Business Suite 12.1 arbeiten, können Sie auch das Szenario 3 anwenden.

Szenario 1:

Um sicherzustellen, dass der Oracle E-Business Suite Konnektor Operationen für Benutzerkonten im Zielsystem ausführen kann, nutzen Sie den Benutzer **APPS** als Synchronisationsbenutzer.

Szenario 2:

Wenn der Benutzer **APPS** nicht direkt als Synchronisationsbenutzer genutzt werden kann, legen Sie einen Synchronisationsbenutzer mit den erforderlichen Minimalberechtigungen an. Nutzen Sie dafür das mitgelieferte Skript und das Wrapper-Package. Die Dateien finden Sie auf dem One Identity Manager-Installationsmedium im Verzeichnis `Modules\EBS\dvd\AddOn\SDK`.

Um den Synchronisationsbenutzer anzulegen

1. Legen Sie das Wrapper-Package `FND_USER_Wrapper.sql` im APPS-Schema Ihrer Oracle Database an.
2. Legen Sie den Synchronisationsbenutzer mit den Minimalberechtigungen an. Nutzen Sie dafür das Skript `CreateSyncUser.sql`.

   Beachten Sie dabei die Anmerkungen im Skript zum Ersetzen der Variablen `&&username` und `&&password`.

Das Skript legt einen Benutzer mit den benötigten Berechtigungen an. Der Wrapper sorgt dafür, dass der Benutzer auch die impliziten Berechtigungen für das Package `apps.fnd_user_pkg` erhält.

Szenario 3:

Wenn Sie weder Szenario 1 noch Szenario 2 anwenden können, dann erstellen Sie einen Synchronisationsbenutzer mit allen benötigten Berechtigungen.

WICHTIG: Der Synchronisationsbenutzer benötigt:

- alle aufgelisteten Rechte

  und zusätzlich
- alle **impliziten** Rechte für das Package `apps.fnd_user_pkg`

Detaillierte Informationen zum Thema

- Benötigte Berechtigungen für die Synchronisation mit einer Oracle E-Business Suite auf Seite 164

Einrichten des Synchronisationsservers

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.

Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem Oracle E-Business Suite Konnektor installiert werden.

Detaillierte Informationen zum Thema

- Systemanforderungen für den Synchronisationsserver auf Seite 17
- One Identity Manager Service installieren auf Seite 17

Systemanforderungen für den Synchronisationsserver

Für die Einrichtung der Synchronisation mit einer Oracle E-Business Suite 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.

Der Synchronisationsserver benötigt eine gute Netzwerkanbindung zum Datenbankserver der Oracle E-Business Suite.

One Identity Manager Service installieren

Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem Oracle E-Business Suite Konnektor installiert sein. Außerdem muss der Synchronisationsserver im One Identity Manager als Jobserver bekannt sein.

Tabelle 3: Eigenschaften des Jobservers

Eigenschaft	Wert
Serverfunktion	Oracle E-Business Suite Konnektor
Maschinenrolle	Server | Jobserver | Oracle E-Business Suite

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 **E-Business Suite**.
5. Auf der Seite **Serverfunktionen** wählen Sie **Oracle E-Business Suite 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 einer Oracle E-Business Suite

Verwenden Sie den Synchronization Editor, um die Synchronisation zwischen One Identity Manager-Datenbank und der Oracle E-Business Suite einzurichten. Nachfolgend sind die Schritte für die initiale Einrichtung eines Synchronisationsprojektes für Benutzerkonten und Berechtigungen beschrieben. Ausführliche Informationen zur Einrichtung der Synchronisation finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

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.

Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

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

Tabelle 4: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Server	Bezeichnung des Servers, auf dem die Oracle Database installiert ist. Es kann der vollqualifizierte Servername oder die IP-Adresse angegeben werden.
Port und Servicename	Port der Oracle Instanz und Bezeichnung des Service.
Benutzer und Kennwort	Benutzername und Kennwort, mit dem sich der Oracle E-Business Suite Konnektor an der Oracle Database anmeldet. Stellen Sie einen Benutzer mit ausreichenden Berechtigungen bereit. Weitere Informationen finden Sie unter Bereitstellen eines Synchronisationsbenutzers auf Seite 15.
Datenquelle	TNS Alias Name aus der `TNSNames.ora`. Diese Angabe wird nur benötigt, wenn der Oracle E-Business Suite Konnektor nur über Oracle Client Software auf die Oracle Database zugreifen kann.
Synchronisationsserver für die Oracle E-Business Suite	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. Weitere Informationen finden Sie unter Einrichten des Synchronisationsservers auf Seite 16.
Verbindungsdaten zur One Identity Manager-Datenbank	• Datenbankserver • Datenbank • SQL Server Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser

Angaben	Erläuterungen
	Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
Remoteverbindungsserver	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 • Oracle E-Business Suite Konnektor ist installiert Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt. Ausführliche Informationen zum Herstellen einer Remoteverbindung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Initiales Synchronisationsprojekt erstellen

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.

HINWEIS: Pro Zielsystem und genutzter Standardprojektvorlage kann genau ein Synchronisationsprojekt erstellt werden.

HINWEIS: Wenn das Synchronisationsprojekt für ein Zielsystem eingerichtet werden soll, das bereits in der One Identity Manager-Datenbank existiert, stellen Sie sicher, dass in der Synchronisationskonfiguration derselbe Server und derselbe eindeutige Name für den DN angegeben wird, wie im bereits vorhandenen Synchronisationsprojekt.

- Verwenden Sie beim Einrichten des Synchronisationsprojekts eine vorhandene Systemverbindung mit der benötigten Konfiguration.

  - ODER -

- Prüfen Sie im Manager den definierten Namen und den Anzeigenamen des E-Business Suite Systems, für welches das Synchronisationsprojekt erstellt werden soll. Folgende Werte müssen übereinstimmen:
  - Anzeigename: **Oracle Finance auf <Server>**
  - Definierter Name: **O=ORA-System,DC=<Eindeutiger Name für den DN>**

Um ein initiales Synchronisationsprojekt für eine Oracle E-Business Suite einzurichten

1. Starten Sie das Launchpad und 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 **Zielsytemtyp Oracle E-Business Suite** 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 **Verbindung herstellen** erfassen Sie die Verbindungsparameter, die der Oracle E-Business Suite Konnektor zur Anmeldung an der Oracle Database benötigt.

Tabelle 5: Anmeldeinformationen für die Verbindung zur Oracle E-Business Suite

Eigenschaft	Beschreibung
Direktzugriff (ohne Oracle Client)	Angabe, ob der Oracle E-Business Suite Konnektor direkt auf die Oracle Database zugreifen kann. Für den Zugriff über Oracle Client Software deaktivieren Sie die Option. Die erforderlichen Verbindungsdaten sind abhängig von der Einstellung dieser Option.
Server	Bezeichnung des Servers auf dem die Oracle Database installiert ist. Es kann der vollqualifizierte Servername oder die IP-Adresse angegeben werden.
Port	Port der Oracle Instanz.
Servicename	Bezeichnung des Service.
Benutzer	Benutzername, mit dem sich der Konnektor an der Oracle Database anmeldet.
Kennwort	Kennwort für die Anmeldung an der Oracle Database.
Datenquelle	TNS Alias Name aus der `TNSNames.ora`.

Die Verbindung zur Oracle Database wird getestet, sobald Sie **Weiter** klicken.

5. Auf der Seite **Verbindungskonfiguration** konfigurieren Sie weitere Standardparameter für die Verbindung.

Tabelle 6: Verbindungskonfiguration

Eigenschaft	Beschreibung
Sprachauswahl	Sprache, die verwendet wird, um Beschreibungstexte aus der Datenbank zu laden.
Eindeutiger Name für den DN	Namensteil, der verwendet wird, um einen eindeutigen definierten Namen für alle Objekte dieses Systems zu generieren. Lassen Sie die Angabe leer, um den Servernamen des Datenbankservers zu nutzen. Dieser Name sollte nach der initialen Synchronisation nicht mehr geändert werden.
Verbindung nur lesend nutzen	Gibt an, ob der Oracle E-Business Suite Konnektor nur lesend auf das Zielsystem zugreifen soll.
Package für Benutzerkonten-Operationen	Name des Wrapper-Packages oder des User-Packages, das zum Anlegen und Ändern von Benutzerkonten und Berechtigungen verwendet werden soll. Syntax: `<Owner>.<PackageName>`

Eigenschaft	Beschreibung
	Abhängig davon, über welches Szenario der Synchronisationsbenutzer erstellt wurde, wird folgende Angabe benötigt: • Benutzer **APPS** (Szenario 1): Keine Angabe erforderlich. Standard ist `APPS.FND_User_PKG`. • Wrapper (Szenario 2): Name des Wrapper-Packages. Standard ist `APPS.FND_USER_WRAPPER`. • Sonst (Szenario 3): Name des User-Packages. Standard ist `APPS.FND_User_PKG`.

6. Auf der Seite **Anzeigename** erfassen Sie einen eindeutigen Anzeigenamen für die Verbindungskonfiguration.

   Über den Anzeigenamen können Sie die Verbindungskonfigurationen für verschiedene Oracle E-Business Suite Verbindungen im Synchronization Editor unterscheiden. Er kann nachträglich nicht mehr geändert werden.

7. Auf der letzten Seite des Systemverbindungsassistenten können Sie die Verbindungsdaten speichern.
   - Aktivieren Sie die Option **Verbindung lokal speichern**, um die Verbindungsdaten zu speichern. Diese können Sie bei der Einrichtung weiterer Synchronisationsprojekte nutzen.
   - Um den Systemverbindungsassistenten zu beenden und zum Projektassistenten zurückzukehren, klicken Sie **Fertig**.

8. 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.

9. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.

10. Auf der Seite **Projektvorlage auswählen** wählen Sie **Oracle E-Business Suite Synchronisation**.

    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.

11. 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.

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

    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.

Verwandte Themen

- Synchronisationsprotokoll konfigurieren auf Seite 28
- Anpassen einer Synchronisationskonfiguration auf Seite 29
- Projektvorlage für Benutzerkonten und Berechtigungen auf Seite 167
- Synchronisationsprojekt für Personendaten erstellen auf Seite 26
- Synchronisationsprojekt für organisatorische Daten erstellen auf Seite 27

Synchronisationsprojekt für Personendaten erstellen

Für die Synchronisation von Daten aus dem Human Resources Modul einer Oracle E-Business Suite erstellen Sie ein separates Synchronisationsprojekt. Dafür wird eine eigene Projektvorlage bereitgestellt.

HINWEIS: Wenn das Synchronisationsprojekt für ein Zielsystem eingerichtet werden soll, das bereits in der One Identity Manager-Datenbank existiert, stellen Sie sicher, dass in der Synchronisationskonfiguration derselbe Server und derselbe eindeutige Name für den DN angegeben wird, wie im bereits vorhandenen Synchronisationsprojekt.

- Verwenden Sie beim Einrichten des Synchronisationsprojekts eine vorhandene Systemverbindung mit der benötigten Konfiguration.

  - ODER -

- Prüfen Sie im Manager den definierten Namen und den Anzeigenamen des E-Business Suite Systems, für welches das Synchronisationsprojekt erstellt werden soll. Folgende Werte müssen übereinstimmen:
  - Anzeigename: **Oracle Finance auf <Server>**
  - Definierter Name: **O=ORA-System,DC=<Eindeutiger Name für den DN>**

Um ein Synchronisationsprojekt für Personendaten einzurichten

- Erstellen Sie ein initiales Synchronisationsprojekt. Es gilt folgende Besonderheit:

  Wählen Sie im Projektassistenten auf der Seite **Projektvorlage auswählen** die Projektvorlage **Oracle E-Business Suite HR-Daten**.

Detaillierte Informationen zum Thema

- Initiales Synchronisationsprojekt erstellen auf Seite 22
- Projektvorlage für HR-Daten auf Seite 168

Verwandte Themen

- Synchronisation von Abteilungen konfigurieren auf Seite 34

Synchronisationsprojekt für organisatorische Daten erstellen

Für die Synchronisation von organisatorischen Daten, wie Lieferanten-Kontaktdaten oder Beteiligte, erstellen Sie eigene Synchronisationsprojekte. Dafür werden separate Projektvorlagen bereitgestellt.

HINWEIS: Wenn auf einer One Identity Manager Datenbank beide Synchronisationsprojekte eingerichtet sind, kann es vorkommen, dass nach der Synchronisation Objekte doppelt vorhanden sind.

Erstellen Sie je One Identity Manager Datenbank nur eines der beiden Synchronisationsprojekte.

HINWEIS: Wenn das Synchronisationsprojekt für ein Zielsystem eingerichtet werden soll, das bereits in der One Identity Manager-Datenbank existiert, stellen Sie sicher, dass in der Synchronisationskonfiguration derselbe Server und derselbe eindeutige Name für

den DN angegeben wird, wie im bereits vorhandenen Synchronisationsprojekt.

- Verwenden Sie beim Einrichten des Synchronisationsprojekts eine vorhandene Systemverbindung mit der benötigten Konfiguration.

  - ODER -

- Prüfen Sie im Manager den definierten Namen und den Anzeigenamen des E-Business Suite Systems, für welches das Synchronisationsprojekt erstellt werden soll. Folgende Werte müssen übereinstimmen:
  - Anzeigename: **Oracle Finance auf <Server>**
  - Definierter Name: **O=ORA-System,DC=<Eindeutiger Name für den DN>**

Um ein Synchronisationsprojekt für Lieferanten-Kontaktdaten einzurichten

- Erstellen Sie ein initiales Synchronisationsprojekt. Es gilt folgende Besonderheit:

  Wählen Sie im Projektassistenten auf der Seite **Projektvorlage auswählen** die Projektvorlage **Oracle E-Business Suite CRM-Daten**.

Um ein Synchronisationsprojekt für Beteiligten-Personendaten einzurichten

- Erstellen Sie ein initiales Synchronisationsprojekt. Es gilt folgende Besonderheit:

  Wählen Sie im Projektassistenten auf der Seite **Projektvorlage auswählen** die Projektvorlage **Oracle E-Business Suite OIM-Daten**.

Detaillierte Informationen zum Thema

- Initiales Synchronisationsprojekt erstellen auf Seite 22
- Projektvorlage für CRM-Daten auf Seite 169
- Projektvorlage für OIM-Daten auf Seite 169

Synchronisationsprotokoll konfigurieren

Im Synchronisationsprotokoll werden alle Informationen, Hinweise, Warnungen und Fehler, die bei der Synchronisation auftreten, aufgezeichnet. Welche Informationen aufgezeichnet werden sollen, kann für jede Systemverbindung separat konfiguriert werden.

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

1. Um das Synchronisationsprotokoll für die Zielsystemverbindung zu konfigurieren, wählen Sie im Synchronization Editor die Kategorie **Konfiguration | Zielsystem**.

   - ODER -

Um das Synchronisationsprotokoll für die Datenbankverbindung zu konfigurieren, wählen Sie im Synchronization Editor die Kategorie **Konfiguration | One Identity Manager Verbindung**.

2. Wählen Sie den Bereich **Allgemein** und klicken Sie **Konfigurieren**.
3. Wählen Sie den Bereich **Synchronisationsprotokoll** und aktivieren Sie **Synchronisationsprotokoll erstellen**.
4. 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.
5. Klicken Sie **OK**.

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.

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 50

Anpassen einer Synchronisationskonfiguration

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

Um die Datenbank und die Oracle E-Business Suite 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 Oracle E-Business Suite Objekte und One Identity Manager-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 E-Business Suite Systeme eingerichtet werden. Hinterlegen Sie die Verbindungsparameter zur Anmeldung an dem jeweiligen System 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 zusätzliche Schemaeigenschaften zu synchronisieren, aktualisieren Sie das Schema im Synchronisationsprojekt. Nehmen Sie die Schemaerweiterungen in das Mapping auf.
- Um zusätzliche Anweisungen für die Initialisierung der Datenbankverbindung zu definieren, bearbeiten Sie die Zielsystemverbindung.
- Um Daten zu synchronisieren, für die keine Schematypen im Konnektorschema angelegt sind, legen Sie eigene Schematypen an. Nehmen Sie die Schemaerweiterungen in das Mapping auf.

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

Detaillierte Informationen zum Thema

- Synchronisation in die Oracle E-Business Suite konfigurieren auf Seite 31
- Synchronisation verschiedener Oracle E-Business Suite Systeme konfigurieren auf Seite 32
- Schema aktualisieren auf Seite 33
- Spezielle Anweisungen für die Datenbankinitialisierung nutzen auf Seite 36
- Weitere Schematypen nutzen auf Seite 36

Wichtige Hinweise für die Anpassung bestehender Synchronisationsprojekte

Wenn die Konfiguration von bereits bestehenden Synchronisationsprojekten angepasst werden soll, prüfen Sie, welche Auswirkungen die Änderungen auf die bereits synchronisierten Daten haben können. Beachten Sie insbesondere die folgenden Hinweise.

Hinweise für die Synchronisation von E-Business Suite Personendaten

Wenn Sie die Mappings für die Synchronisation von Personendaten unternehmensspezifisch anpassen, prüfen Sie, ob auch die zu sperrenden Spalten an der Tabelle `Person` oder

Locality angepasst werden müssen. Um weitere Spalten für die Bearbeitung im One Identity Manager zu sperren, hinterlegen Sie an der Tabelle Person oder Locality kundenspezifische Skripte (OnLoaded).

Ausführliche Informationen zu Tabellenskripten finden Sie im *One Identity Manager Konfigurationshandbuch*.

Anpassen der Verbindungsparameter zur Oracle E-Business Suite

Die Verbindungsparameter zum Zielsystem können nachträglich über den Systemverbindungsassistenten geändert werden.

Der eindeutige Name für den DN wird verwendet, um einen eindeutigen definierten Namen für alle Objekte des Systems zu generieren. Wenn dieser nach der initialen Synchronisation geändert wird, können bei der nächsten Synchronisation die Objekte nicht mehr eindeutig identifiziert werden. Damit werden alle Objekte erneut in der One Identity Manager-Datenbank angelegt.

Der eindeutige Name für den DN sollte nach der initialen Synchronisation nicht geändert werden.

Wenn der eindeutige Name für den DN vor der initialen Synchronisation geändert werden muss, muss diese Änderung zusätzlich in die Variable CP_EBSSystemDN übernommen werden. Diese Variable wird in der Filterbedingung für den Scope verwendet.

Ausführliche Informationen zur Anpassung der Verbindungsparameter und zur Bearbeitung von Variablen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Synchronisation in die Oracle E-Business Suite 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**.

HINWEIS: Nur Synchronisationsprojekte, die mit der Projektvorlage **Oracle E-Business Suite Synchronisation** erstellt wurden, enthalten einen Provisionierungsworkflow.

Um eine Synchronisationskonfiguration für die Synchronisation in die Oracle E-Business Suite 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 Oracle E-Business Suite Systeme konfigurieren auf Seite 32

Synchronisation verschiedener Oracle E-Business Suite Systeme konfigurieren

Unter bestimmten Voraussetzungen ist es möglich ein Synchronisationsprojekt für die Synchronisation verschiedener E-Business Suite Systeme zu nutzen.

Voraussetzungen

- Die Zielsystemschemas der E-Business Suite Systeme sind identisch.
- Alle virtuellen Schemaeigenschaften, die im Mapping genutzt werden, müssen in den erweiterten Schemas der E-Business Suite Systeme vorhanden sein.
- Die Verbindungsparameter zum Zielsystem sind als Variablen hinterlegt.

Um ein Synchronisationsprojekt für die Synchronisation eines weiteren Systems anzupassen

1. Stellen Sie in dem weiteren System einen Benutzer für den Zugriff auf die Oracle E-Business Suite mit ausreichenden Berechtigungen bereit.
2. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
3. Erstellen Sie für das weitere System ein neues Basisobjekt. Verwenden Sie den Assistenten zur Anlage eines Basisobjektes.
   - Wählen Sie im Assistenten den Oracle E-Business Suite 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 Oracle E-Business Suite konfigurieren auf Seite 31

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. Wählen Sie die Kategorie **Mappings**.
2. 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.

Synchronisation von Abteilungen konfigurieren

Für die Synchronisation von Abteilungen und Mitgliedschaften in Abteilungen werden die Daten aus den Schematypen `HROrganization` und `HRPersonInOrganization` ausgelesen. Für die Synchronisation dieser Daten sollten die benötigten Objekte gefiltert werden. Andernfalls kann die Synchronisation aller Abteilungen die Synchronisationsperformance deutlich beeinträchtigen.

Wenn Sie die Standardmappings dieser Schematypen nutzen, können Sie die benötigten Abteilungen aus der Organisationshierarchie auswählen. Bearbeiten Sie dafür den Scope des Synchronisationsprojekts und erstellen Sie Hierarchiefilter.

Abteilungen können außerdem durch ihren Typ von anderen Organisationen unterschieden werden. Da diese Typen in der Oracle E-Business Suite kundenspezifisch definiert werden können, werden die Abteilungen in den Standardmappings nicht nach dem Typ gefiltert. Um Abteilungen über ihren Typ zu filtern, definieren Sie eigene Schemaklassen.

Wenn Sie kundenspezifische Mappings für die Synchronisation von Abteilungen nutzen, definieren Sie die Filter bereits an den Schemaklassen. Zusätzlich können Sie den Hierarchiefilter nutzen, um die Menge der Synchronisationsobjekte weiter einzuschränken.

Verwandte Themen

- Synchronisationsprojekt für Personendaten erstellen auf Seite 26

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.

Oracle E-Business Suite unterstützt die Revisionsfilterung. Als Revisionszähler wird das Datum der letzten Änderung der E-Business Suite 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 E-Business Suite 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.

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**.

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

Spezielle Anweisungen für die Datenbankinitialisierung nutzen

An der Zielsystemverbindung können verschiedene zusätzliche Einstellungen vorgenommen werden, wenn die Konfiguration des Zielsystems das erfordert. Beispielsweise kann die Standard-Sprach- und Uhrzeitformatierung durch eine SQL-Anweisung überschrieben werden, die bei jedem Verbindungsaufbau ausgeführt wird.

Um zusätzliche Anweisungen für die Datenbankinitialisierung zu nutzen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Aktivieren Sie den Expertenmodus.
3. Bearbeiten Sie die Zielsystemverbindung.
    a. Wählen Sie die Kategorie **Konfiguration | Zielsystem**.
    b. Klicken Sie **Verbindung bearbeiten**.

       Der Systemverbindungsassistent wird gestartet.
    c. Wählen Sie die Seite **Datenbankverbindungsinitialisierung** und geben Sie SQL-Anweisungen an, die bei jedem Verbindungsaufbau ausgeführt werden sollen.
    d. Klicken Sie **Prüfen**.
    e. Beenden Sie den Systemverbindungsassistenten.

       Die Verbindungsparameter werden aktualisiert.
4. Speichern Sie die Änderungen.

SQL-Anweisungen können bereits beim Einrichten eines Synchronisationsprojekts angegeben werden, wenn der Synchronization Editor im Expertenmodus ausgeführt wird.

Weitere Schematypen nutzen

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 38.
3. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
4. Aktivieren Sie den Expertenmodus.
5. Wählen Sie die Kategorie **Konfiguration | Zielsystem**.
6. Klicken Sie **Verbindung bearbeiten**.

   Der Systemverbindungsassistent wird gestartet.
7. Prüfen Sie die erfassten Daten.
8. Auf der Seite **Schemadefinition (manuell)** erfassen Sie 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**.
9. Um den Systemverbindungsassistenten zu beenden, klicken Sie **Fertig**.
10. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
11. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

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

    Die Schematypen werden in der Liste der ungenutzten Schematypen angezeigt.
13. 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*.

14. 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*.
15. Speichern Sie die Änderungen.
16. Führen Sie eine Konsistenzprüfung durch.
17. Aktivieren Sie das Synchronisationsprojekt.

Um den Schemaanteil der Schemaerweiterungsdatei aus dem Konnektorschema zu entfernen

1. Entfernen Sie alle Mappings und Synchronisationsschritte, welche für die zusätzlichen Schematypen angelegt wurden.
2. Bearbeiten Sie die Zielsystemverbindung mit dem Systemverbindungsassistenten.
    - Auf der Seite **Schemadefinition (manuell)** klicken Sie **Vorhandene entfernen**.
3. Aktualisieren Sie das Schema.
4. Speichern Sie die Änderungen.
5. Führen Sie eine Konsistenzprüfung durch.
6. 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 für die neuen Schematypen. Hier definierte Schematypen werden immer dem vorhandenen Schema hinzugefügt. Wenn ein neuer Schematyp denselben Namen hat, wie ein bereits vorhandener Schematyp, wird die Erweiterung ignoriert.

Es kann nur eine einzige Schemaerweiterungsdatei angegeben werden. Darin müssen alle gewünschten Erweiterungen erfasst sein. Wird zu einer Verbindungskonfiguration, die bereits eine Schemaerweiterungsdatei enthält, erneut eine Schemaerweiterungsdatei hinzugefügt, so wird die vorherige Definition überschrieben.

Die Schemaerweiterungsdatei definiert Schematypen als Objekte, daher entspricht der grundsätzliche Aufbau einer Liste von Objektdefinitionen. Eine Objektdefinition enthält die Definition eines Schematypes. Eine Datei kann beliebig viele Objektdefinitionen enthalten.

Struktur der Schemaerweiterungsdatei

```
<?xml version="1.0" encoding="utf-8" ?>
<EBSF12>
```

```
    <ObjectNames>
        <Object>
            ...
        <\Object>
    <\ObjectNames>
</EBSF12>
```

Detaillierte Informationen zum Thema

- Objektdefinitionen auf Seite 39
- Tabellendefinitionen auf Seite 41
- Methodendefinitionen auf Seite 43
- Beispiel für eine Schemaerweiterungsdatei auf Seite 176

Objektdefinitionen

Die Objektdefinitionen dienen der formalen Beschreibung, aus welchen Quellen, mit welchen Schlüsselwerten und mit welchen Bedingungen Datenobjekte eines Schematyps selektiert werden. Diese formale Beschreibung wird vom Oracle E-Business Suite Konnektor ausgewertet und es werden SQL-Anweisungen zur Datenbankanfrage daraus generiert. Da es zulässig ist, Daten für ein Objekt eines Schematyps aus mehreren Tabellen zu ermitteln, ist es notwendig, Tabellen- und Spaltennamen stets in der vollständigen Namensnotation `<Schemaname>.<Tabellenname>.<Spaltenname>` zu verwenden.

Beispiel: `AK.AK_ATTRIBUTES_TL.ATTRIBUTE_CODE`

Tabelle 7: Attribute einer Objektdefinition

Attribut	Beschreibung
SchemaName	Frei gewählter Name des zu definierenden Schematyps. Unter diesem Namen werden die Objekte dieses Typs im erweiterten Schema angezeigt.
ParentSchemaName	Bezug zu einem weiteren Schematyp, der in der Hierarchie übergeordnet ist. Beispiel: `Application` ist `ParentSchemaName` von `Attribute`
DisplayPattern	Definition eines Anzeigemusters für die Anzeige der Objekte im Synchronization Editor (beispielsweise im Zielsystembrowser oder bei der Definition der Schemaklassen).
IsReadOnly	Gibt an, ob die Objekte dieses Schematyps nur gelesen werden können. Der Standardwert ist **false**.
AddRootDN	Gibt an, ob der eindeutige Name für den DN an den definierten

Attribut	Beschreibung
	Namen aller Objekte dieses Schematyps angefügt werden soll. Der Standardwert ist **true**.
UseDistinct	Gibt an, ob doppelte Einträge durch Anwendung der `Distinct`-Funktion verhindert werden sollen. Der Standartwert ist **false**.

Beispiel

```
<Object SchemaName="ORA-Attribute" ParentSchemaName="ORA-Application"
DisplayPattern="%AK.AK_ATTRIBUTES_TL.ATTRIBUTE_CODE%" IsReadOnly="true"
UseDistinct="false" >
```

Objektschlüsseldefinition

Der Objektschlüssel definiert alle Spalten, die notwendig sind, um genau ein Objekt des Schematyps zu selektieren. Zur Definition der Schlüsselspalten werden `<Key>`-Tags verwendet. Das Tag `<ObjektKey>` umschließt eine beliebige Anzahl von `<Key>`-Tags. Damit werden die Bestandteile des eindeutigen Schlüssels für alle Elemente eines Schematyps deklariert und die Spalten benannt, die für die Identifikation eines Einzelobjektes dieses Schematyps benötigt werden. Die korrekte Angabe aller Schlüsselspalten ist sowohl für die Selektion der Einzelobjekte als auch für mögliche `Join`-Operationen wichtig.

Tabelle 8: Attribute einer Objektschlüsseldefinition

Attribut	Beschreibung
Column	Name der Spalte in vollständiger Namensnotation.
IsReferencedColumn	Gibt an, ob die Schlüsselspalte für eine Referenzauflösung von anderen Schematypen benötigt wird. Der Standardwert ist **false**.
IsDNColumn	Gibt an, ob der Wert dieser Spalte als Bestandteil in den definierten Namen des Objekts eingefügt wird. Der Standardwert ist **false**.
X500Abbreviation	Kürzel, welches dem Wert aus dieser Spalte bei der Bildung des definierten Namen vorangestellt wird. Nur benötigt, wenn `IsDNColumn="true"`.

Beispiel

```
<Objectkey>
    <Key Column="APPLSYS.FND_APPLICATION.APPLICATION_ID" IsDNColumn="true"
    X500Abbreviation="AP" />
</Objectkey>
```

Tabellendefinitionen

Das Tag <Tables> umschließt eine beliebige Anzahl von Tabellendefinitionen in <Table>-Tags. Damit ist es möglich, alle Tabellen oder Views zu benennen, aus denen Daten für ein Einzelobjekt dieses Schematyps benötigt werden. Die grundlegend notwendigen Informationen zu einer Tabelle werden in den Attributen des <Table>-Tags definiert.

Tabelle 9: Attribute einer Tabellendefinition

Attribut	Beschreibung
Name	Name der Tabelle (ohne Schemaname).
Schema	Name des Oracle Schemas.
APK	Name einer Spalte, die alternativer Primärschlüssel sein kann. Diese Spalte wird stets mit geladen.
USN	Name einer Spalte, welche die Information über die letzte Änderung der Objekte trägt. Wenn die Spalte LAST_UPDATE_DATE vorhanden ist, wird sie standardmäßig als Änderungsinformation genutzt und muss nicht explizit angegeben werden.
WhereClause	Where–Klausel zur Einschränkung der Ergebnismenge.
JoinParentColumn	Kommagetrennte Liste von Spalten in einer übergeordneten Tabelle, wenn eine Join–Operation zu einem hierarchisch übergeordneten Schematyp ausgeführt werden soll (vollständige Notation).
JoinChildColumn	Kommagetrennte Liste von Spalten in der aktuell definierten Tabelle, die in der Join–Operation mit den Spalten aus JoinParentColumn verbunden werden sollen (vollständige Notation). Die Reihenfolge der Spalten in den Listen bestimmt, welche Spalten miteinander verbunden werden.

Beispiel

```
<Tables>
    <Table Name="FND_RESPONSIBILITY_TL" Schema="APPLSYS" APK="" USN=""
    WhereClause="APPLSYS.FND_RESPONSIBILITY_TL.LANGUAGE='US'"
    JoinParentColumn="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID,APPLSYS.FND_
    RESPONSIBILITY.APPLICATION_ID" JoinChildColumn="APPLSYS.FND_RESPONSIBILITY_
    TL.RESPONSIBILITY_ID,APPLSYS.FND_RESPONSIBILITY_TL.APPLICATION_ID" >
</Tables>
```

Definition der Primärschlüssel

Die <PK>-Tags innerhalb der <Table>-Sektion benennen die Primärschlüsselspalten einer Tabelle. Der Name der Spalte wird dabei im Attribut Column angegeben. Um mehrspaltige

Primärschlüssel zu definieren, geben Sie jede Spalte in einem eigenen Tag an. Es können beliebig viele <PK>-Tags in einer Tabellendefinition verwendet werden.

Tabelle 10: Attribut einer Primärschlüsseldefinition

Attribut	Beschreibung
Column	Name der Primärschlüsselspalte.

Beispiel

```
<PK Column="REQUEST_GROUP_ID" />
```

Spaltenpaare in der Hierarchie

Die <ParentTableFK>-Tags innerhalb der <Table>-Sektion beschreiben die Spaltenpaare, die bei einer Join-Operation mit der Tabelle des hierarchisch übergeordneten Schematyps gleichzusetzen sind.

Tabelle 11: Attribute eines Spaltenpaars

Attribut	Beschreibung
Column	Name der Spalte in der aktuell definierten Tabelle.
ParentColumn	Name der Spalte in der Tabelle des übergeordneten Schematyps.

Beispiel

```
<ParentTableFK Column="APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID"
ParentColumn="APPLSYS.FND_APPLICATION.APPLICATION_ID" />
```

Beispiel einer vollständigen Tabellendefinition

```
<Object SchemaName="ORA-Responsibility" ParentSchemaName="ORA-Application"
DisplayPattern="%vrtDistinguishedName%" IsReadOnly="true" UseDistinct="false">
    <ObjectKey>
        <Key Column="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID"
        IsDNColumn="true" IsReferencedColumn="true" X500Abbreviation="RE" />
        <Key Column="APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID" />
    </ObjectKey>
    <Tables>
        <Table Name="FND_RESPONSIBILITY" Schema="APPLSYS" APK="" USN=""
        WhereClause="" JoinParentColumn="" JoinChildColumn="" >
            <PK Column="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID" />
```

```
            <ParentTableFK Column="APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID"
            ParentColumn="APPLSYS.FND_APPLICATION.APPLICATION_ID" />
        </Table>
        <Table Name="FND_RESPONSIBILITY_TL" Schema="APPLSYS" APK=""
        USN="APPLSYS.FND_RESPONSIBILITY_TL.LAST_UPDATE_DATE"
        WhereClause="APPLSYS.FND_RESPONSIBILITY_TL.LANGUAGE='$SYSLANGU$'"
        JoinParentColumn="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID,APPLSYS.FND_
        RESPONSIBILITY.APPLICATION_ID" JoinChildColumn="APPLSYS.FND_RESPONSIBILITY_
        TL.RESPONSIBILITY_ID,APPLSYS.FND_RESPONSIBILITY_TL.APPLICATION_ID" >
            <PK Column="APPLSYS.FND_RESPONSIBILITY_TL.RESPONSIBILITY_ID" />
        </Table>
        <Table Name="FND_APPLICATION" Schema="APPLSYS" APK="" USN="" WhereClause=""
        JoinParentColumn="APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID"
        JoinChildColumn="APPLSYS.FND_APPLICATION.APPLICATION_ID" >
            <PK Column="APPLSYS.FND_APPLICATION.APPLICATION_ID" />
        </Table>
    </Tables>
</Object>
```

Erläuterungen

Die vorstehende Definition zeigt die Deklaration des Schematyps `ORA-Responsibility`, wie sie vom Oracle E-Business Suite Konnektor intern verwendet wird.

Der Schematyp ist hierarchisch dem Schematyp `ORA-Application` untergeordnet (`ParentSchemaName`). Er hat zwei Objektschlüsselspalten (`APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID` und `APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID`), von denen nur eine als Bestandteil in den definierten Namen aufgenommen wird `IsDNColumn="true"`. Die Spalte `APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID` ist Bestandteil des `DistinguishedName` des übergeordneten Schematyps, der automatisch hinten angefügt wird.

Zur Selektion aller Eigenschaften werden Sätze aus den Tabellen `FND_RESPONSIBILITY`, `FND_RESPONSIBILITY_TL` und `FND_APPLICATION` mittels `Join`-Operation angefragt. Die Spalten für die `Join`-Operation sind jeweils in den Attributen `JoinParentColumn` und `JoinChildColumn` angegeben.

Der Beschreibungstext wird in der von der Datenbank-Verbindungskonfiguration vorgegebenen Sprache aus der Tabelle `FND_RESPONSIBILITY_TL` gelesen. Dafür wird in der Where-Klausel die symbolische Variable `$SYSLANGU$` genutzt. Weitere Informationen finden Sie unter Symbolische Variablen in Where-Klauseln auf Seite 46.

Methodendefinitionen

Mit dem `<Functions>`-Tag ist es innerhalb einer Objektdefinition möglich, Methoden zu definieren, die für Objekte des Schematyps ausführbar sind. Jede Methode führt beliebig

viele SQL-Funktionen aus.

Die Benennung des XML-Tags für eine Methode bestimmt den Methodennamen. Innerhalb der Methoden-Sektion werden eine oder mehrere Funktionen definiert. Diese Funktionen werden in einer festgelegten Reihenfolge ausgeführt, wenn an einem Objekt des Schematyps die entsprechende Methode aufgerufen wird.

Struktur der Methodendefinitionen

```
<Functions>
      <Insert>
            <Function ... OrderNumber="1" >
                  <Parameter ...>
            </Function>
            <Function ... OrderNumber="2" >
                  <Parameter ...>
            </Function>
      </Insert>
      <Delete>
            <Function ...>
                  <Parameter ...>
            </Function>
      </Delete>
</Functions>
```

Im Beispiel hat der Schematyp zwei Methoden, `Insert` und `Delete`. Beim Aufruf von `Insert` sind zwei Funktionen auszuführen, die durch ihr `OrderNumber`-Attribut in eine feste Reihenfolge gebracht werden. Beim Aufruf der `Delete`-Methode wird nur eine definierte Funktion ausgeführt.

Funktionsdefinitionen

Die `<Function>`-Sektion definiert Name, Ausführungsreihenfolge und Parametrisierung von SQL-Funktionsaufrufen.

Tabelle 12: Attribute einer Funktionsdefinition

Attribut	Beschreibung
Name	Name der Funktion. Vollständige Notation in der Form `<Schemaname>.<Paketname>.<Funktionsname>`.
OrderNumber	Numerische Angabe der Ausführungsreihenfolge. Der Standardwert ist **1**.

Eine Sonderstellung nimmt dabei das Funktionspaket ein, welches Funktionen zur Modifikation von Benutzerkonten bereitstellt (APPS.FND_USER_PKG). Aufgrund der Berechtigungseinschränkungen bei der Ausführung von Funktionen dieses Paketes kann es notwendig sein, ein Wrapper-Paket zu implementieren, welches den Aufrufkontext ändert. Der Name dieses Wrapper-Paketes kann in der Verbindungskonfiguration gespeichert werden. Er wird zur Laufzeit vor der Ausführung der Funktion in dem SQL-Block ersetzt. Die symbolische Variable für den definierten Paketnamen lautet $ebsUserPackageName$. Weitere Informationen finden Sie unter Initiales Synchronisationsprojekt erstellen auf Seite 22.

Beispiel

```
<Function Name="$ebsUserPackageName$.CreateUser" OrderNumber="1" >
```

Parameterdefinitionen

Die <Parameter>-Tags definieren die an eine Funktion zu übergebenden Parameter, deren Typ und die Quelle des Parameterwertes.

Tabelle 13: Attribute einer Parameterdefinition

Attribut	Beschreibung
Name	Name des Parameters in der Funktionsdefinition.
PropertyName	Name der Objekteigenschaft, deren Wert übergeben werden soll (vollständige Notation). - ODER - Festwert, wenn PropertyType="FIX" definiert ist.
PropertyType	Datentyp. Mögliche Werte sind: • **CHAR**: Zeichenkette. • **DATE**: Datumswert. Der Wert wird als gültiges Datum konvertiert. • **FIX**: Fester Stringwert. Es wird immer der im Attribut PropertyName angegebene Festwert übergeben. • **NUM**: Numerischer Wert. Die Konvertierung lässt keine alpha-numerischen Zeichen zu.
Mandatory	Gibt an, ob der Parameter ein Pflichtparameter ist. Der Standardwert ist **false**.
NullValue	Wert oder Zeichenkette, die als Null-Wert übergeben werden soll. Diese Angabe ist notwendig, um Parameter mit speziell in Funktionspaketen definierten oder in Oracle Database allgemein bekannten Werten als Null-Repräsentation zu bestücken. Die Angabe dieses Attributes ist optional. Als Standard wird bei Erkennung eines Null-Wertes auf einem Pflichtparameter die Zeichenkette **null** übergeben. Ein optionaler

Attribut	Beschreibung
	Parameter wird in diesem Fall nicht an den Funktionsaufruf übergeben. In drei Fällen ist eine Null-Wert-Definition sinnvoll: a. Verwendung einer im Funktionspaket definierten Konstante, beispielsweise **$ebsUserPackageName$.null_number**. Hierbei würde der Name des in der Verbindungskonfiguration gespeicherten Funktionspaketes zur Benutzerkonten-Modifikation eingesetzt, sofern der variable Ausdruck `$ebsUserPackageName$` erkannt wird. b. Verwendung einer in der Oracle Database definierten symbolischen Konstante, beispielsweise **sysdate**. c. Verwendung eines speziellen Ausdrucks ungleich **null**, beispielsweise **to_date('-2', 'J')**.

Beispiel

```
<Parameter Name="start_date" PropertyName="APPS.FND_USER_RESP_GROUPS_DIRECT.START_
DATE" PropertyType="DATE" Mandatory="TRUE" NullValue="sysdate" />
```

Symbolische Variablen in Where-Klauseln

Zu jeder Konfiguration einer Datenbankverbindung zu einer Oracle E-Business Suite gehört die Einstellung der Sprachversion. Die aus der Datenbank geladenen Texte sollen in der eingestellten Sprachversion geliefert werden, sofern die Texte übersetzt sind. Diese Einstellung kann mit der symbolischen Variable `$SYSLANGU$` in Where-Klauseln genutzt werden. Die Variable wird vor der Ausführung der SQL-Anweisung durch den tatsächlich eingestellten Wert ersetzt.

Beispiel

```
<Table Name="FND_SECURITY_GROUPS_TL" Schema="APPLSYS" APK="" USN=""
WhereClause="APPLSYS.FND_SECURITY_GROUPS_TL.LANGUAGE='$SYSLANGU$'"
JoinParentColumn="APPLSYS.FND_SECURITY_GROUPS.SECURITY_GROUP_ID"
JoinChildColumn="APPLSYS.FND_SECURITY_GROUPS_TL.SECURITY_GROUP_ID" >
```

Einzelobjektsynchronisation konfigurieren

Änderungen an einem einzelnen Objekt im Zielsystem können sofort in die One Identity Manager-Datenbank übertragen werden, ohne dass eine vollständige Synchronisation der Zielsystem-Umgebung gestartet werden muss. Die Einzelobjektsynchronisation kann nur für Objekte ausgeführt werden, die in der One Identity Manager-Datenbank bereits vorhanden sind. Es werden die Änderungen an den gemappten Objekteigenschaften

übernommen. Gehört zu diesen Objekteigenschaften eine Mitgliederliste, werden auch die Einträge in der Zuordnungstabelle aktualisiert. Ist das Objekt im Zielsystem nicht mehr vorhanden, wird es in der One Identity Manager-Datenbank gelöscht.

Voraussetzungen

- Es gibt einen Synchronisationsschritt, der die Änderungen am geänderten Objekt in den One Identity Manager einlesen kann.
- Für die Tabelle, die das geänderte Objekt enthält, ist der Pfad zum Basisobjekt der Synchronisation festgelegt.

Für Synchronisationsprojekte, die mit der Standard-Projektvorlage erstellt wurden, ist die Einzelobjektsynchronisation vollständig konfiguriert. Wenn Sie kundenspezifische Tabellen in solch ein Synchronisationsprojekt einbeziehen möchten, müssen Sie die Einzelobjektsynchronisation für diese Tabellen konfigurieren. Ausführliche Informationen dazu finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Um den Pfad zum Basisobjekt der Synchronisation für eine kundenspezifische Tabelle festzulegen

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Oracle E-Business Suite**.
3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die kundenspezifische Tabelle zu, für die Sie die Einzelobjektsynchronisation nutzen möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die kundenspezifische Tabelle und erfassen Sie den **Pfad zum Basisobjekt**.

   Geben Sie den Pfad zum Basisobjekt in der ObjectWalker-Notation der VI.DB an.

   Beispiel: `FK(UID_EBSSystem).XObjectKey`
8. Speichern Sie die Änderungen.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 52
- Ausstehende Objekte nachbearbeiten auf Seite 52

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 **Oracle E-Business Suite Konnektor** zu.

   Alle Jobserver müssen auf das gleiche E-Business Suite System 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

- E-Business Suite Jobserver bearbeiten auf Seite 157

Ausführen einer Synchronisation

Synchronisationen werden über zeitgesteuerte Prozessaufträge gestartet. Im Synchronization Editor ist es auch möglich, eine Synchronisation manuell zu starten. Zuvor können Sie die Synchronisation simulieren, um das Ergebnis der Synchronisation abzuschätzen und Fehler in der Synchronisationskonfiguration aufzudecken. Wenn eine Synchronisation irregulär abgebrochen wurde, müssen Sie die Startinformation zurücksetzen, um die Synchronisation erneut starten zu können.

Wenn verschiedene Zielsysteme immer in einer vorher festgelegten Reihenfolge synchronisiert werden sollen, nutzen Sie Startfolgen, um die Synchronisation zu starten. In einer Startfolge können beliebige Startkonfigurationen aus verschiedenen Synchronisationsprojekten zusammengestellt und in eine Ausführungsreihenfolge gebracht werden. Ausführliche Informationen zu Startfolgen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Detaillierte Informationen zum Thema

- Synchronisationen starten auf Seite 49
- Synchronisationen deaktivieren auf Seite 51
- Synchronisationsergebnisse anzeigen auf Seite 50

Synchronisationen starten

Beim Einrichten des initialen Synchronisationsprojekts über das Launchpad wird ein Standardzeitplan für regelmäßige Synchronisationen erstellt und zugeordnet. Um regelmäßige Synchronisationen auszuführen, aktivieren Sie diesen Zeitplan.

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**.

Wenn kein Zeitplan aktiviert ist, können Sie die Synchronisation auch manuell starten.

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**.

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.

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.

Verwandte Themen

- Synchronisationsprotokoll konfigurieren auf Seite 28
- Fehleranalyse auf Seite 55

Synchronisationen deaktivieren

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**.

Einzelobjekte synchronisieren

Die Einzelobjektsynchronisation kann nur für Objekte ausgeführt werden, die in der One Identity Manager-Datenbank bereits vorhanden sind. Es werden die Änderungen an den gemappten Objekteigenschaften übernommen. Gehört zu diesen Objekteigenschaften eine Mitgliederliste, werden auch die Einträge in der Zuordnungstabelle aktualisiert.

HINWEIS:Ist das Objekt im Zielsystem nicht mehr vorhanden, wird es in der One Identity Manager-Datenbank gelöscht.

Um ein Einzelobjekt zu synchronisieren

1. Wählen Sie im Manager die Kategorie **E-Business Suite**.
2. Wählen Sie in der Navigationsansicht den Objekttyp.
3. Wählen Sie in der Ergebnisliste das Objekt, das Sie synchronisieren möchten.
4. Wählen Sie die Aufgabe **Objekt synchronisieren**.

   Es wird ein Prozess zum Lesen dieses Objekts in die Jobqueue eingestellt.

Detaillierte Informationen zum Thema

- Einzelobjektsynchronisation konfigurieren auf Seite 46

Aufgaben nach einer Synchronisation

Nach der Synchronisation von Daten aus dem Zielsystem in die One Identity Manager-Datenbank können Nacharbeiten erforderlich sein. Prüfen Sie folgende Aufgaben:

- Ausstehende Objekte nachbearbeiten auf Seite 52

Ausstehende Objekte nachbearbeiten

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 **Oracle E-Business Suite | Zielsystemabgleich: Oracle E-Business Suite**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp **Oracle E-Business Suite** 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 14: 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. 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 .

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.

Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen

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

Um Tabellen in den Zielsystemabgleich aufzunehmen

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Oracle E-Business Suite**.
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.

Verwandte Themen

- Ausstehende Objekte nachbearbeiten auf Seite 52

Fehleranalyse

Bei der Analyse und Behebung von Synchronisationsfehlern unterstützt Sie der Synchronization Editor auf verschiedene Weise.

- Synchronisation simulieren

  Die Simulation ermöglicht es, das Ergebnis einer Synchronisation abzuschätzen. Dadurch können beispielsweise Fehler in der Synchronisationskonfiguration aufgedeckt werden.

- Synchronisation analysieren

  Für die Analyse von Problemen während der Synchronisation, beispielsweise unzureichender Performance, kann der Synchronisationsanalysebericht erzeugt werden.

- Meldungen protokollieren

  Der One Identity Manager bietet verschiedene Möglichkeiten zur Protokollierung von Meldungen. Dazu gehören das Synchronisationsprotokoll, die Protokolldatei des One

Identity Manager Service, die Protokollierung von Meldungen mittels NLog und weitere.

- Startinformation zurücksetzen

  Wenn eine Synchronisation irregulär abgebrochen wurde, beispielsweise weil ein Server nicht erreichbar war, muss die Startinformation manuell zurückgesetzt werden. Erst danach kann die Synchronisation erneut gestartet werden.

- Revision zurücksetzen

  Mitunter kann es erforderlich sein, bei der Synchronisation auch solche Objekte zu verarbeiten, deren Änderungsinformation seit der letzten Synchronisation nicht erneuert wurde. Das kann beispielsweise notwendig sein, wenn Datenänderungen vorgenommen wurden, ohne dass die Änderungsinformation am Objekt aktualisiert wurde. Dadurch ist die Änderungsinformation an den Objekten nun älter als die in der Synchronisationskonfiguration gespeicherte Revision. In solchen Fällen kann die Revision für eine Startkonfiguration zurückgesetzt werden.

Ausführliche Informationen zu diesen Themen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 50

3

Managen von E-Business Suite Benutzerkonten und Personen

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 E-Business Suite System, 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. 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.

Wenn Personendaten aus dem HR Modul der Oracle E-Business Suite im One Identity Manager abgebildet werden, können die importierten Personen

- als HR Personen an E-Business Suite Benutzerkonten zugeordnet werden,
- über die automatische Personenzuordnung, über Kontendefinitionen oder manuell mit Benutzerkonten verbunden werden.

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

Verwandte Themen

- Einrichten von Kontendefinitionen auf Seite 58
- Automatische Zuordnung von Personen zu E-Business Suite Benutzerkonten auf Seite 76
- Stammdaten für E-Business Suite Benutzerkonten erfassen auf Seite 129
- Verbinden von E-Business Suite Benutzerkonten mit importierten Personen auf Seite 82

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 E-Business Suite 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:

- Kontendefinitionen erstellen
- Automatisierungsgrade erstellen
- Abbildungsvorschriften für IT Betriebsdaten erstellen
- IT Betriebsdaten erfassen

- Zuweisen der Kontendefinitionen an Personen
- (Optional) Kontendefinitionen an Zielsysteme zuweisen

Kontendefinitionen erstellen

Um eine Kontendefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | 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.

Stammdaten von Kontendefinitionen

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 15: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet.
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. Für ein E-Business Suite System lassen Sie die Angabe leer.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatisierungsgrad (initial)	Standardautomatisierungsgrad, der bei Neuanlage von Benutzerkonten standardmäßig verwendet werden soll.
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

Eigenschaft	Beschreibung
	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 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 deaktiviert.

Eigenschaft	Beschreibung
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 deaktiviert.
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 deaktiviert.
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 deaktiviert.
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.

Automatisierungsgrade erstellen

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 **Oracle E-Business Suite | 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 **Oracle E-Business Suite | 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.

Stammdaten von Automatisierungsgraden

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 16: 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. • **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	Angabe, ob die Benutzerkonten zum Löschen markierter

Eigenschaft	Beschreibung
verzögertem Löschen beibehalten	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.

Verwandte Themen

- Ungültige Berechtigungszuweisungen auf Seite 122

Abbildungsvorschriften für IT Betriebsdaten erstellen

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 **Oracle E-Business Suite | 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 17: 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.
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 | EBS | Accounts | MailTemplateDefaultValues** an.

4. Speichern Sie die Änderungen.

IT Betriebsdaten erfassen

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 A. Zusätzlich erhalten einige Personen der Abteilung A administrative Benutzerkonten A.

Erstellen Sie eine Kontendefinition A für die Standardbenutzerkonten A und eine Kontendefinition B für die administrativen Benutzerkonten 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 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 18: 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 **Oracle E-Business Suite | 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 Kontendefinitionen 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, deaktiviert.

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

Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | 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.

Kontendefinitionen an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | 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.

Kontendefinitionen an alle Personen zuweisen

Um eine Kontendefinition an alle Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | 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.

Kontendefinitionen direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | 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.

Kontendefinitionen 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 **Oracle E-Business Suite | 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.

Kontendefinitionen 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 **Oracle E-Business Suite | 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 **Oracle E-Business Suite | 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 **Oracle E-Business Suite | 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 **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 von Kontendefinitionen auf Seite 59

Kontendefinitionen an Zielsysteme zuweisen

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**).

Um die Kontendefinition an ein Zielsystem zuzuweisen

1. Wählen Sie im Manager in der Kategorie **Oracle E-Business Suite | Systeme** das System.
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.

Detaillierte Informationen zum Thema

- Automatische Zuordnung von Personen zu E-Business Suite Benutzerkonten auf Seite 76

Kontendefinitionen löschen

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 **Oracle E-Business Suite | 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 **Oracle E-Business Suite | 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 **Oracle E-Business Suite | 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 **Oracle E-Business Suite | 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 **Oracle E-Business Suite | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

      - ODER -

      Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen** (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 **Oracle E-Business Suite | 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 **Oracle E-Business Suite | Systeme** das System.
   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 **Oracle E-Business Suite | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
   b. Wählen Sie in der Ergebnisliste die Kontendefinition.
   c. Klicken Sie , um die Kontendefinition zu löschen.

Automatische Zuordnung von Personen zu E-Business Suite Benutzerkonten

Beim Einfügen eines Benutzerkontos kann automatisch eine vorhandene Person zugeordnet werden. 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 | EBS | PersonAutoFullsync** und wählen Sie den gewünschten Modus.
- Wenn Personen außerhalb der Synchronisation zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | EBS | PersonAutoDefault** und wählen Sie den gewünschten Modus.
- Legen Sie im Konfigurationsparameter **TargetSystem | EBS | PersonExcludeList** die Benutzerkonten fest, für die keine automatische Zuordnung zu Personen erfolgen soll.

  Beispiel:

  ```
  ANONYMOUS|SYSADMIN|AUTOINSTALL|INITIAL SETUP|FEEDER SYSTEM|CONCURRENT
  ```
- Legen Sie über den Konfigurationsparameter **TargetSystem | EBS | PersonAutoDisabledAccounts** fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
- Weisen Sie dem E-Business Suite System eine Kontendefinition zu. Stellen Sie sicher, dass der Automatisierungsgrad, der verwendet werden soll, als Standardautomatisierungsgrad eingetragen ist.
- Definieren Sie die Suchkriterien für die Personenzuordnung an diesem System.

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.

Ausführliche Informationen zur automatischen Personenzuordnung finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Kontendefinitionen erstellen auf Seite 59
- Kontendefinitionen an Zielsysteme zuweisen auf Seite 73
- Automatisierungsgrad an Benutzerkonten ändern auf Seite 81
- Suchkriterien für die automatische Personenzuordnung bearbeiten auf Seite 78

Suchkriterien für die automatische Personenzuordnung bearbeiten

Die Kriterien für die Personenzuordnung werden am E-Business Suite System 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 `EBSSystem` 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 **Oracle E-Business Suite | Systeme**.
2. Wählen Sie in der Ergebnisliste das E-Business Suite System.
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 19: Standardsuchkriterien für Benutzerkonten

Anwenden auf	Spalte an Person	Spalte am Benutzerkonto
E-Business Suite Benutzerkonten	E-Business Suite Benutzerkonto (`CentralEBSAccount`)	Benutzername (`UserName`)
	Person (`UID_Person`)	HR Person (`UID_PersonEmployee`)

5. Speichern Sie die Änderungen.

Ausführliche Informationen zur Definition der Suchkriterien finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Automatische Zuordnung von Personen zu E-Business Suite Benutzerkonten auf Seite 76
- Personen suchen und direkt an Benutzerkonten zuordnen auf Seite 79

Personen suchen und direkt an Benutzerkonten zuordnen

Anhand der Suchkriterien können Sie eine Vorschlagsliste für die Personenzuordnung an Benutzerkonten erzeugen und die Zuordnung direkt ausführen. Die Benutzerkonten sind dafür in verschiedenen Ansichten zusammengestellt.

Tabelle 20: 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 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.

Um Suchkriterien auf die Benutzerkonten anzuwenden

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | Systeme**.
2. Wählen Sie in der Ergebnisliste das E-Business Suite System.
3. Wählen Sie die Aufgabe **Suchkriterien für die Personenzuordnung definieren**.
4. Im unteren Bereich des Formulars klicken Sie **Neu laden**.

   Für alle Benutzerkonten im Zielsystem werden die möglichen Zuordnungen anhand der Suchkriterien ermittelt. Die drei Ansichten werden aktualisiert.

TIPP: Mit Maus-Doppelklick auf einen Eintrag in den Ansichten werden das Benutzerkonto und die Person geöffnet und Sie können die Stammdaten einsehen.

Durch die Zuordnung von Personen an die Benutzerkonten entstehen verbundene Benutzerkonten (Zustand **Linked**). Um verwaltete Benutzerkonten zu erhalten (Zustand **Linked configured**), können Sie gleichzeitig eine Kontendefinition zuordnen.

Um Personen direkt über die Vorschlagsliste zuzuordnen

- Klicken Sie **Vorgeschlagene Zuordnungen**.
    1. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die vorgeschlagene Person zugeordnet werden soll. Eine Mehrfachauswahl ist möglich.
    2. (Optional) Wählen Sie im Auswahlfeld **Diese Kontendefinition zuweisen** eine Kontendefinition und im Auswahlfeld **Diesen Automatisierungsgrad zuweisen** einen Automatisierungsgrad.
    3. Klicken Sie **Ausgewählte zuweisen.**
    4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

       Den ausgewählten Benutzerkonten werden die per Suchkriterium ermittelten Personen zugeordnet. Wenn eine Kontendefinition ausgewählt wurde, wird diese an alle ausgewählten Benutzerkonten zugeordnet.

  - ODER -

- Klicken Sie **Ohne Personenzuordnung**.
    1. Klicken Sie **Person auswählen** für das Benutzerkonto, dem eine Person zugeordnet werden soll. Wählen Sie eine Person aus der Auswahlliste.
    2. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die ausgewählten Personen zugeordnet werden sollen. Eine Mehrfachauswahl ist möglich.
    3. (Optional) Wählen Sie im Auswahlfeld **Diese Kontendefinition zuweisen** eine Kontendefinition und im Auswahlfeld **Diesen Automatisierungsgrad zuweisen** einen Automatisierungsgrad.
    4. Klicken Sie **Ausgewählte zuweisen**.
    5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

       Den ausgewählten Benutzerkonten werden die Personen zugeordnet, die in der Spalte **Person** angezeigt werden. Wenn eine Kontendefinition ausgewählt wurde, wird diese an alle ausgewählten Benutzerkonten zugeordnet.

Um Zuordnungen zu entfernen

- Klicken Sie **Zugeordnete Benutzerkonten**.
    1. Klicken Sie **Auswahl** für alle Benutzerkonten, deren Personenzuordnung entfernt werden soll. Mehrfachauswahl ist möglich.
    2. Klicken Sie **Ausgewählte entfernen**.
    3. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

       Von den ausgewählten Benutzerkonten werden die zugeordneten Personen entfernt.

Automatisierungsgrad an Benutzerkonten ändern

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 **Oracle E-Business Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Automatisierungsgrad** den Automatisierungsgrad.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für E-Business Suite Benutzerkonten auf Seite 129

Kontendefinitionen an verbundene Benutzerkonten zuweisen

An Benutzerkonten im Zustand **Linked** (verbunden) kann nachträglich eine Kontendefinition zugewiesen werden. Das kann beispielsweise der Fall sein, wenn

- Personen und Benutzerkonten manuell verbunden wurden
- die automatische Personenzuordnung konfiguriert ist, beim Einfügen eines Benutzerkontos jedoch noch keine Kontendefinition am E-Business Suite System zugeordnet ist

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie dem System eine Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand **Linked** (verbunden) die Kontendefinition und den Automatisierungsgrad zu.
    a. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | Benutzerkonten | Verbunden aber nicht konfiguriert | <System>**.

b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.

Detaillierte Informationen zum Thema

- Kontendefinitionen an Zielsysteme zuweisen auf Seite 73

Personen manuell mit E-Business Suite Benutzerkonten verbinden

Eine Person kann mit mehreren E-Business Suite Benutzerkonten verbunden werden, beispielsweise um zusätzlich zum Standardbenutzerkonto ein administratives Benutzerkonto zuzuweisen. Darüber hinaus kann eine Person Standardbenutzerkonten mit verschiedenen Typen nutzen.

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.

Um einer Person manuell Benutzerkonten zuzuweisen

1. Wählen Sie die Kategorie **Personen | Personen**.
2. Wählen Sie in der Ergebnisliste die Person und führen Sie die Aufgabe **E-Business Suite Benutzerkonten zuweisen** aus.
3. Weisen Sie die Benutzerkonten zu.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Unterstützte Typen von Benutzerkonten auf Seite 85

Verbinden von E-Business Suite Benutzerkonten mit importierten Personen

Aus der Oracle E-Business Suite importierte Personendaten werden in der One Identity Manager-Datenbank in der Tabelle `Person` abgebildet. An jeder importierten Person ist die Datenquelle des Imports angegeben (Spalte `ImportSource`). An den E-Business Suite Benutzerkonten gibt es verschiedene Eigenschaften, über die diese Personen zugeordnet werden können.

Um eine importierte Person an ein Benutzerkonto zuzuordnen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Allgemein**.
5. Wählen Sie aus der Auswahlliste **HR Person** die HR Person.

   - ODER -

   Wählen Sie aus der Auswahlliste **Kunde** den Kunden.

   - ODER -

   Wählen Sie aus der Auswahlliste **Lieferant** den Lieferanten.
6. Speichern Sie die Änderungen.

Solange die importierten Personen nur über diese Spalten mit den Benutzerkonten verbunden sind, werden die Benutzerkonten nicht über den One Identity Manager verwaltet. Wird eine Person deaktiviert oder als sicherheitsgefährdend eingestuft, hat diese Änderung keine Auswirkung auf das zugeordnete Benutzerkonto. Um die Möglichkeiten des One Identity Manager zur Verwaltung von Benutzerkonten und Personen für die importierten Personen zu nutzen, erstellen Sie verbundene Benutzerkonten. Dabei werden die Personen über die Spalte `EBSUser.UID_Person` mit den Benutzerkonten verbunden.

HR Personen können zusätzlich über die automatische Personenzuordnung mit Benutzerkonten verbunden werden. Dafür sind Standardsuchkriterien definiert.

Tabelle 21: An Benutzerkonten zugeordnete Personen

Eigenschaft	Beschreibung
Person (`UID_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. Es kann jede aktive Person zugeordnet werden.
Kunde (`UID_PersonCustomer`)	Verweis auf eine Person, die als Kunde geführt ist. Es können nur Personen aus der Datenquelle **E-Business Suite AR** zugeordnet werden (`Person.ImportSource='EBSOIM'`).
HR Person (`UID_PersonEmployee`)	Verweis auf eine Person im Human Resources Modul der Oracle E-Business Suite. Es können nur Personen aus der Datenquelle **E-Business Suite HR** zugeordnet werden (`Person.ImportSource='EBSHR'`).
Beteiligter	Verweis auf eine Person, die als Beteiligter geführt ist.

Eigenschaft	Beschreibung
(UID_PersonParty)	Es kann eine Person mit der Datenquelle **E-Business Suite AR** zugeordnet sein (Person.ImportSource='EBSOIM'). Die Zuordnung kann im One Identity Manager nicht bearbeitet werden.
Lieferant (UID_PersonSupplier)	Verweis auf eine Person, die als Lieferant oder Kontakt geführt ist. Es können nur Personen aus der Datenquelle **E-Business Suite AP** zugeordnet werden (Person.ImportSource='EBSCRM').

Detaillierte Informationen zum Thema

- Managen von E-Business Suite Benutzerkonten und Personen auf Seite 57
- Suchkriterien für die automatische Personenzuordnung bearbeiten auf Seite 78

Verwandte Themen

- Synchronisationsprojekt für Personendaten erstellen auf Seite 26
- Synchronisationsprojekt für organisatorische Daten erstellen auf Seite 27
- HR Personen auf Seite 147
- Beteiligte auf Seite 149
- Lieferanten und Kontakte auf Seite 148

Besonderheiten beim Löschen von Personen

Wenn in der One Identity Manager-Datenbank eine Person gelöscht wird, die mit einem E-Business Suite Benutzerkonto verbunden ist, verliert das Benutzerkonto nach Ablauf der Löschverzögerung seine Referenz auf die Person. Wenn das Benutzerkonto über eine Kontendefinition verwaltet wird, ist das Verhalten beim Löschen der verbundenen Person an der Kontendefinition festgelegt. Benutzerkonten können im One Identity Manager nicht gelöscht werden. Die Person wird physisch aus der One Identity Manager-Datenbank gelöscht, sobald alle übrigen Voraussetzungen zum Löschen gegeben sind. Das Benutzerkonto bleibt mit dem Status **INACTIVE** erhalten.

Ausführliche Informationen zum Löschen von Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- E-Business Suite Benutzerkonten löschen auf Seite 137
- E-Business Suite Benutzerkonten deaktivieren auf Seite 136

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 22: 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.

Detaillierte Informationen zum Thema

- Standardbenutzerkonten auf Seite 86
- Administrative Benutzerkonten auf Seite 87
- Privilegierte Benutzerkonten auf Seite 88

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.

Verwandte Themen

- Einrichten von Kontendefinitionen auf Seite 58

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.

Verwandte Themen

- Nutzungsberechtigte Personen an ein Benutzerkonto mit Gruppenidentität zuweisen auf Seite 90

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.

- Um ein Präfix für den Anmeldenamen zu verwenden, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | EBS | Accounts | PrivilegedAccount | AccountName_Prefix**.
- Um ein Postfix für den Anmeldenamen zu verwenden, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | EBS | Accounts | PrivilegedAccount | AccountName_Postfix**.

Diese Konfigurationsparameter werden in der Standardinstallation ausgewertet, wenn Sie ein Benutzerkonto, mit der Eigenschaft **Privilegiertes Benutzerkonto** (Spalte `IsPrivilegedAccount`) kennzeichnen. Die Anmeldenamen der Benutzerkonten werden entsprechend der Bildungsregeln umbenannt. Dies erfolgt auch, wenn die Benutzerkonten

über den Zeitplan **Ausgewählte Benutzerkonten als privilegiert kennzeichnen** als privilegiert gekennzeichnet werden.

Verwandte Themen

- Einrichten von Kontendefinitionen auf Seite 58

Nutzungsberechtigte Personen an ein Benutzerkonto mit Gruppenidentität zuweisen

Weisen Sie einem administrativen Benutzerkonto mit einer Gruppenidentität die Personen zu, die das Benutzerkonto im Zielsystem nutzen. Es können nur Personen mit der Identität **Primäre Identität** zugewiesen werden.

Um Personen mit Nutzungsberechtigungen zuzuweisen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto mit einer Gruppenidentität.
3. Wählen Sie die Aufgabe **Personen mit Nutzungsberechtigungen zuzuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

   - ODER -

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

4

Bereitstellen von Anmeldeinformationen

Wenn neue Benutzerkonten im One Identity Manager angelegt werden, werden sofort auch die zur Anmeldung am Zielsystem benötigten Kennwörter erstellt. Um das initiale Kennwort zu vergeben, stehen verschiedene Möglichkeiten zur Verfügung. Auf die Kennwörter werden vordefinierte Kennwortrichtlinien angewendet, die Sie bei Bedarf an Ihre Anforderungen anpassen können. Um die generierten Anmeldeinformationen an die Benutzer zu verteilen, können Sie E-Mail-Benachrichtigungen einrichten.

Detaillierte Informationen zum Thema

- Kennwortrichtlinien für E-Business Suite Benutzerkonten auf Seite 91
- Initiales Kennwort für neue E-Business Suite Benutzerkonten auf Seite 102
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 103

Kennwortrichtlinien für E-Business Suite 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 92
- Kennwortrichtlinien anwenden auf Seite 93

- Kennwortrichtlinien bearbeiten auf Seite 95
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 98
- Ausschlussliste für Kennwörter bearbeiten auf Seite 101
- Kennwörter prüfen auf Seite 101
- Generieren von Kennwörtern testen auf Seite 102

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.

Für E-Business Suite Systeme ist die Kennwortrichtlinie **Oracle E-Business Suite Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Benutzerkonten (`EBSUser.Password`) eines E-Business Suite Systems anwenden.

Wenn die Kennwortanforderungen der E-Business Suite Systeme unterschiedlich sind, wird empfohlen, je System eine eigene Kennwortrichtlinie einzurichten.

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

Kennwortrichtlinien anwenden

Für E-Business Suite Systeme ist die Kennwortrichtlinie **Oracle E-Business Suite Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Benutzerkonten (`EBSUser.Password`) eines E-Business Suite Systems anwenden.

Wenn die Kennwortanforderungen der E-Business Suite Systeme unterschiedlich sind, wird empfohlen, je System 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 E-Business Suite Systems 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 **Oracle E-Business Suite | 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 23: 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 **Oracle E-Business Suite | 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.

Kennwortrichtlinien bearbeiten

Um eine Kennwortrichtlinie zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | 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 95
- Richtlinieneinstellungen auf Seite 96
- Zeichenklassen für Kennwörter auf Seite 97
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 98

Allgemeine Stammdaten einer Kennwortrichtlinie

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 24: 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,

Eigenschaft	Bedeutung
	wenn die Richtlinie nicht erfüllt wird. Übersetzen Sie den eingegebenen Text über die Schaltfläche .
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 25: 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

Eigenschaft	Bedeutung
	im Kennwortrücksetzungsportal zurückgesetzt werden. Ausführliche Informationen finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.
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 26: 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.

Eigenschaft	Bedeutung
Min. Anzahl Ziffern	Angabe, wie viele Ziffern ein Kennwort mindestens enthalten muss.
Min. Anzahl Sonderzeichen	Angabe, wie viele Sonderzeichen ein Kennwort mindestens enthalten muss.
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 99
- Skript zum Generieren eines Kennwortes auf Seite 100

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 **Oracle E-Business Suite | 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 100

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 **Oracle E-Business Suite | 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 99

Ausschlussliste für Kennwörter bearbeiten

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.

Kennwörter prüfen

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 **Oracle E-Business Suite | 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 von Kennwörtern 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 **Oracle E-Business Suite | 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 E-Business Suite Benutzerkonten

Um das initiale Kennwort für neue E-Business Suite 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 | EBS | 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 E-Business Suite Benutzerkonten auf Seite 91
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 103

E-Mail-Benachrichtigungen über Anmeldeinformationen

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 zu nutzen, sind folgende Voraussetzungen zu erfüllen:

- Stellen Sie sicher, dass das E-Mail-Benachrichtungssystem im One Identity Manager konfiguriert ist. Ausführliche Informationen finden Sie im *One Identity Manager Installationshandbuch*.
- Aktivieren Sie im Designer den Konfigurationsparameter **Common | MailNotification | DefaultSender** und geben Sie die Absenderadresse an, mit der die E-Mail Benachrichtigungen verschickt werden.
- 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*.
- 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 | EBS | Accounts | InitialRandomPassword**.
2. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | EBS | Accounts | InitialRandomPassword | SendTo** und erfassen Sie als Wert den Empfänger der Benachrichtigung.

   Ist kein Empfänger ermittelbar, dann wird die E-Mail an die im Konfigurationsparameter **TargetSystem | EBS | DefaultAddress** hinterlegte Adresse versandt.
3. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | EBS | 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 | EBS | 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

Managen von Berechtigungszuweisungen

E-Business Suite Benutzerkonten erhalten ihre Berechtigungen auf die Objekte einer Oracle E-Business Suite über Zuständigkeiten. Dabei können Zuständigkeiten nicht direkt an die Benutzerkonten zugewiesen werden, sondern werden über Sicherheitsgruppen vererbt. Berechtigungen in der Oracle E-Business Suite sind durch die Kombination aus Zuständigkeiten und Sicherheitsgruppen charakterisiert. Diese Kombinationen werden in der One Identity Manager-Datenbank als E-Business Suite Berechtigungen abgebildet.

In der Oracle E-Business Suite können Berechtigungen direkt und indirekt an Benutzerkonten zugewiesen sein. Dabei können mehrere indirekte Zuweisungen mit unterschiedlichen Gültigkeitszeiträumen existieren. Indirekte Zuweisungen werden in den One Identity Manager eingelesen und können für Auswertungen und Berichte genutzt werden. Direktzuweisungen werden ebenfalls eingelesen. Für jedes Benutzerkonto kann es nur genau eine Direktzuweisung geben.

Im One Identity Manager können E-Business Suite Berechtigungen ebenfalls direkt oder indirekt zugewiesen werden. Berechtigungszuweisungen, die im One Identity Manager vorgenommen werden, werden als Direktzuweisungen in die Oracle E-Business Suite provisioniert. Dazu wird aus allen Berechtigungszuweisungen für ein Benutzerkonto die Zuweisung mit dem effektiven Gültigkeitszeitraum ermittelt.

In der One Identity Manager-Datenbank werden direkte und indirekte Berechtigungszuweisungen folgendermaßen gekennzeichnet.

Tabelle 27: Kennzeichnen von direkten und indirekten Berechtigungszuweisungen in der Tabelle `EBSUserInResp`

Herkunft der Zuweisung	Art der Zuweisung	Indirekt (Spalte `OriginIndirect`)	Herkunft (Spalte `XOrigin`)
Oracle E-Business Suite	indirekt	1 (ja)	1
	direkt	0 (nein)	1

Herkunft der Zuweisung	Art der Zuweisung	Indirekt (Spalte `OriginIndirect`)	Herkunft (Spalte `XOrigin`)
One Identity Manager	direkt	0 (nein)	1
	indirekt	0 (nein)	2
	dynamisch	0 (nein)	4
	Zuweisungsbestellung	0 (nein)	8
	unwirksam	0 (nein)	16

Ausführliche Informationen zur Berechnung von Zuweisungen im One Identity Manager finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Detaillierte Informationen zum Thema

- Zuweisen von E-Business Suite Berechtigungen an Benutzerkonten im One Identity Manager auf Seite 106
- Gültigkeitszeitraum von Berechtigungszuweisungen auf Seite 116

Zuweisen von E-Business Suite Berechtigungen an Benutzerkonten im One Identity Manager

Im One Identity Manager können E-Business Suite Berechtigungen direkt oder indirekt an Personen zugewiesen werden. Bei der indirekten Zuweisung werden Personen und Berechtigungen in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der Berechtigungen, die einer Person zugewiesen ist. Wenn die Person ein E-Business Suite Benutzerkonto besitzt, dann erhält dieses Benutzerkonto die Berechtigungen. Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind:

- Für Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen ist die Zuweisung von Personen und E-Business Suite Berechtigungen erlaubt.
- Die Benutzerkonten sind mit der Option **Berechtigungen erbbar** gekennzeichnet.
- Die Benutzerkonten sind über die Spalte `UID_Person` (**Person**) mit einer Person verbunden.
- Benutzerkonten und E-Business Suite Berechtigungen gehören zum selben E-Business Suite System.

Des Weiteren können Berechtigungen über IT Shop-Bestellungen an Personen zugewiesen werden. Damit Berechtigungen über IT Shop-Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle Berechtigungen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Berechtigungen werden nach erfolgreicher Genehmigung den Personen zugewiesen.

Über Systemrollen können Berechtigungen zusammengefasst und als Paket an Personen zugewiesen werden. Sie können Systemrollen erstellen, die ausschließlich E-Business Suite Berechtigungen enthalten. Ebenso können in einer Systemrolle Systemberechtigungen aus unterschiedlichen Zielsystemen zusammengefasst werden.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die E-Business Suite Berechtigungen auch direkt an Benutzerkonten zuweisen.

Ausführliche Informationen finden Sie in den folgenden Handbüchern.

Thema	Handbuch
Vererbung von Unternehmensressourcen	*One Identity Manager Administrationshandbuch für das Identity Management Basismodul* *One Identity Manager Administrationshandbuch für Geschäftsrollen*
Zuweisung von Unternehmensressourcen über IT Shop-Bestellungen	*One Identity Manager Administrationshandbuch für IT Shop*
Systemrollen	*One Identity Manager Administrationshandbuch für Systemrollen*

Detaillierte Informationen zum Thema

- Gültigkeitszeitraum von Berechtigungszuweisungen auf Seite 116
- E-Business Suite Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 108
- E-Business Suite Berechtigungen an Geschäftsrollen zuweisen auf Seite 109
- E-Business Suite Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 112
- E-Business Suite Berechtigungen in Systemrollen aufnehmen auf Seite 110
- E-Business Suite Berechtigungen in den IT Shop aufnehmen auf Seite 110
- E-Business Suite Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 114

E-Business Suite Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Berechtigung an Abteilungen, Kostenstellen oder Standorte zu, damit sie über diese Organisationen an Benutzerkonten zugewiesen wird.

Um eine Berechtigung an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Berechtigungen**.
2. Wählen Sie in der Ergebnisliste die Berechtigung.
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 Berechtigungen an eine Abteilung, eine Kostenstelle oder einen Standort 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, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe**E-Business Suite Berechtigungen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungen zu.

   - ODER -

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

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer Oracle E-Business Suite auf Seite 9

E-Business Suite Berechtigungen an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie Berechtigungen an Geschäftsrollen zu, damit sie über diese Geschäftsrollen an Benutzerkonten zugewiesen werden.

Um eine Berechtigung an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Berechtigungen**.
2. Wählen Sie in der Ergebnisliste die Berechtigung.
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 Berechtigungen 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 **E-Business Suite Berechtigungen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungen zu.

   - ODER -

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

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer Oracle E-Business Suite auf Seite 9

E-Business Suite Berechtigungen in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

Mit dieser Aufgabe nehmen Sie eine Berechtigung in Systemrollen auf. Wenn Sie eine Systemrolle an Personen zuweisen, wird die Berechtigung an alle Benutzerkonten vererbt, die diese Personen besitzen.

HINWEIS: Berechtigungen, 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 finden Sie im *One Identity Manager Administrationshandbuch für Systemrollen*.

Um eine Berechtigung an Systemrollen zuzuweisen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Berechtigungen**.
2. Wählen Sie in der Ergebnisliste die Berechtigung.
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.

E-Business Suite Berechtigungen in den IT Shop aufnehmen

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

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

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Berechtigung im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.
- Soll die Berechtigung nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss die Berechtigung 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 Berechtigungen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Berechtigungen in den IT Shop aufzunehmen.

Um eine Berechtigung in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | Berechtigungen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | E-Business Suite Berechtigungen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigung an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Berechtigung aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | Berechtigungen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

Um eine Berechtigung aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | Berechtigungen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | E-Business Suite Berechtigungen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

5. Klicken Sie **OK**.

   Die Berechtigung wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Berechtigung 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 für E-Business Suite Berechtigungen auf Seite 138
- One Identity Manager Benutzer für die Verwaltung einer Oracle E-Business Suite auf Seite 9

E-Business Suite Benutzerkonten direkt an eine Berechtigung zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Berechtigungen direkt an Benutzerkonten zuweisen.

Um eine Berechtigung direkt an Benutzerkonten zuzuweisen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Berechtigungen**.
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.

Im oberen Bereich des Formulars werden alle bereits zugewiesenen Benutzerkonten mit ihren Gültigkeitszeiträumen angezeigt. Die Übersicht zeigt sowohl die direkt als auch die indirekt zugewiesenen Benutzerkonten. Für Direktzuweisungen ist ein **Aktiv von (direkt)** Datum gesetzt; indirekte Zuweisungen haben kein direktes Gültigkeitsdatum.

Um die Berechtigung an ein Benutzerkonto zuzuweisen

1. Klicken Sie **Hinzufügen**.
2. Wählen Sie aus der Auswahlliste **Benutzerkonto** das Benutzerkonto.
3. Erfassen Sie im Eingabefeld **Aktiv von (direkt)** den ersten Gültigkeitstag der direkten Berechtigungszuweisung.
4. (Optional) Erfassen Sie im Eingabefeld **Aktiv bis (direkt)** den letzten Gültigkeitstag der direkten Berechtigungszuweisung.
5. (Optional) Fügen Sie weitere Benutzerkonten hinzu.
6. Speichern Sie die Änderungen.

Um eine direkte Berechtigungszuweisung zu bearbeiten

1. Wählen Sie in der Übersicht die direkte Berechtigungszuweisung, die Sie bearbeiten möchten.
2. Ändern Sie die Werte in den Eingabefeldern **Aktiv von (direkt)**, **Aktiv bis (direkt)** oder **Beschreibung**.
3. Speichern Sie die Änderungen.

Es können nur Direktzuweisungen bearbeitet werden. Wenn Sie in der Übersicht eine indirekte Zuweisungen auswählen und bearbeiten, wird dafür zusätzlich eine Direktzuweisung angelegt.

Berechtigungszuweisungen können nicht gelöscht werden. Es gibt stattdessen zwei Möglichkeiten, um zu kennzeichnen, dass eine Direktzuweisung nicht mehr gültig ist.

- Tragen Sie ein Datum als Ablaufdatum der Zuweisung ein.

  Wählen Sie diese Möglichkeit beispielsweise dann, wenn eine Berechtigungszuweisung an einem festgelegten Datum in der Zukunft ungültig werden soll.

  - ODER -

- Entfernen Sie die Berechtigungszuweisung.

  Wählen Sie diese Möglichkeit beispielsweise dann, wenn neben der Direktzuweisung auch eine vererbte Berechtigungszuweisung existiert und die Direktzuweisung durch die vererbte Berechtigungszuweisung ersetzt werden soll.

Um das Ablaufdatum für eine direkte Berechtigungszuweisung zu setzen

1. Wählen Sie in der Übersicht die direkte Berechtigungszuweisung, die nicht mehr wirksam sein soll.
2. Neben dem Eingabefeld **Aktiv bis (direkt)** klicken Sie **...**.
3. Klicken Sie **Heute** oder legen Sie an anderes Ablaufdatum fest.
4. Speichern Sie die Änderungen.

Um eine direkte Berechtigungszuweisung zu entfernen

1. Wählen Sie in der Übersicht die direkte Berechtigungszuweisung, die nicht mehr wirksam sein soll.
2. Klicken Sie **Entfernen**.
3. Speichern Sie die Änderungen.

   Der erste und letzte Gültigkeitstag der Direktzuweisung (**Aktiv von (direkt)** und **Aktiv bis (direkt)**) werden gelöscht. Der letzte Gültigkeitstag (**Aktiv bis (effektiv)**) wird neu berechnet. Wenn es keine gültige Zuweisung mehr gibt, wird der letzte Gültigkeitstag auf ein Datum in der Vergangenheit gesetzt und `XOrigin` erhält den Wert **16**.

Detaillierte Informationen zum Thema

- Gültigkeitszeitraum von Berechtigungszuweisungen auf Seite 116

Verwandte Themen

- Ungültige Berechtigungszuweisungen auf Seite 122

E-Business Suite Berechtigungen direkt an ein Benutzerkonto zuweisen

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

Um Berechtigungen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Berechtigungen zuweisen**.

Im oberen Bereich des Formulars werden alle bereits zugewiesenen Berechtigungen mit ihren Gültigkeitszeiträumen angezeigt. Die Übersicht zeigt sowohl die direkt als auch die indirekt zugewiesenen Berechtigungen. Für Direktzuweisungen ist ein **Aktiv von (direkt)** Datum gesetzt; indirekte Zuweisungen haben kein direktes Gültigkeitsdatum.

Um eine Berechtigung an das Benutzerkonto zuzuweisen

1. Klicken Sie **Hinzufügen**.
2. Wählen Sie aus der Auswahlliste **E-Business Suite Berechtigung** die zuzuweisende Berechtigung.
3. Erfassen Sie im Eingabefeld **Aktiv von (direkt)** den ersten Gültigkeitstag der direkten Berechtigungszuweisung.
4. (Optional) Erfassen Sie im Eingabefeld **Aktiv bis (direkt)** den letzten Gültigkeitstag der direkten Berechtigungszuweisung.
5. (Optional) Fügen Sie weitere Berechtigungen hinzu.
6. Speichern Sie die Änderungen.

Um eine direkte Berechtigungszuweisung zu bearbeiten

1. Wählen Sie in der Übersicht die direkte Berechtigungszuweisung, die Sie bearbeiten möchten.
2. Ändern Sie die Werte in den Eingabefeldern **Aktiv von (direkt)**, **Aktiv bis (direkt)** oder **Beschreibung**.
3. Speichern Sie die Änderungen.

Es können nur Direktzuweisungen bearbeitet werden. Wenn Sie in der Übersicht eine indirekte Zuweisungen auswählen und bearbeiten, wird dafür zusätzlich eine Direktzuweisung angelegt.

Berechtigungszuweisungen können nicht gelöscht werden. Es gibt stattdessen zwei Möglichkeiten, um zu kennzeichnen, dass eine Direktzuweisung nicht mehr gültig ist.

- Tragen Sie ein Datum als Ablaufdatum der Zuweisung ein.

  Wählen Sie diese Möglichkeit beispielsweise dann, wenn eine Berechtigungszuweisung an einem festgelegten Datum in der Zukunft ungültig werden soll.

  - ODER -

- Entfernen Sie die Berechtigungszuweisung.

  Wählen Sie diese Möglichkeit beispielsweise dann, wenn neben der Direktzuweisung auch eine vererbte Berechtigungszuweisung existiert und die Direktzuweisung durch die vererbte Berechtigungszuweisung ersetzt werden soll.

Um das Ablaufdatum für eine direkte Berechtigungszuweisung zu setzen

1. Wählen Sie in der Übersicht die direkte Berechtigungszuweisung, die nicht mehr wirksam sein soll.
2. Neben dem Eingabefeld **Aktiv bis (direkt)** klicken Sie **...**.
3. Klicken Sie **Heute** oder legen Sie an anderes Ablaufdatum fest.
4. Speichern Sie die Änderungen.

Um eine direkte Berechtigungszuweisung zu entfernen

1. Wählen Sie in der Übersicht die direkte Berechtigungszuweisung, die nicht mehr wirksam sein soll.
2. Klicken Sie **Entfernen**.
3. Speichern Sie die Änderungen.

   Der erste und letzte Gültigkeitstag der Direktzuweisung (**Aktiv von (direkt)** und **Aktiv bis (direkt)**) werden gelöscht. Der letzte Gültigkeitstag (**Aktiv bis (effektiv)**) wird neu berechnet. Wenn es keine gültige Zuweisung mehr gibt, wird der letzte Gültigkeitstag auf ein Datum in der Vergangenheit gesetzt und `XOrigin` erhält den Wert **16**.

Detaillierte Informationen zum Thema

- Gültigkeitszeitraum von Berechtigungszuweisungen auf Seite 116

Verwandte Themen

- Ungültige Berechtigungszuweisungen auf Seite 122
- E-Business Suite Berechtigungen in den IT Shop aufnehmen auf Seite 110

Gültigkeitszeitraum von Berechtigungszuweisungen

Berechtigungszuweisungen können zeitlich befristet sein. Ein Benutzerkonto kann seine Berechtigungen sowohl durch Direktzuweisung als auch über verschiedene Vererbungswege erhalten. Jede dieser Zuweisungen kann einen anderen Gültigkeitszeitraum haben. Der One Identity Manager ermittelt aus allen Gültigkeitszeiträumen den zum aktuellen Zeitpunkt effektiv wirksamen Gültigkeitszeitraum. Bei dieser Berechnung werden alle Zuweisungen mit `OriginIndirect = 0` berücksichtigt.

Tabelle 28: Eigenschaften einer Berechtigungszuweisung

Eigenschaft	Beschreibung
Aktiv von (effektiv)	Erster Gültigkeitstag der Zuweisung. Das Datum wird aus allen Zuweisungen (direkten und indirekten) berechnet.
Aktiv bis (effektiv)	Letzter Gültigkeitstag der Zuweisung. Das Datum wird aus allen Zuweisungen (direkten und indirekten) berechnet. Wenn kein Datum angegeben ist, ist die Zuweisung unbefristet.
Aktiv von (direkt)	Erster Gültigkeitstag der Direktzuweisung.
Aktiv bis (direkt)	Letzter Gültigkeitstag der Direktzuweisung. Wenn kein Datum angegeben ist, ist die Zuweisung unbefristet.
Indirekt	Gibt an, ob diese Zuweisung eine indirekte Berechtigung aus dem Zielsystem abbildet. Indirekte Zuweisungen können im One Identity Manager nicht bearbeitet werden.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Berechnung des effektiven Gültigkeitszeitraums

Zu einer Benutzerkonto-Berechtigungs-Kombination kann es im One Identity Manager mehrere Zuweisungen mit unterschiedlichen Gültigkeitszeiträumen geben. In die Oracle E-Business Suite wird jedoch nur die wirksame Zuweisung provisioniert. Dafür berechnet der One Identity Manager aus allen Zuweisungen den effektiven Gültigkeitszeitraum. Die verschiedenen Zuweisungsarten gehen folgendermaßen in die Berechnung ein:

Tabelle 29: Gültigkeitszeitraum ermitteln

Art der Zuweisung	Gültigkeitszeitraum
Direktzuweisung	**Aktiv von (direkt)** und **Aktiv bis (direkt)**
Bestellung	Gültigkeitszeitraum der Bestellung, wenn das

Art der Zuweisung	Gültigkeitszeitraum
	Gültig von Datum der Bestellung erreicht oder überschritten ist. Bei unbefristeten Bestellungen wird der 01.01.1900 als erster Gültigkeitstag gesetzt.
Zuweisungsbestellung	Gültigkeitszeitraum der Bestellung, wenn das **Gültig von** Datum der Bestellung erreicht oder überschritten ist. Bei unbefristeten Bestellungen wird der 01.01.1900 als erster Gültigkeitstag gesetzt.
Vererbung über Abteilung, Standort, Kostenstelle oder Geschäftsrolle (keine Zuweisungsbestellung)	nur unbefristet Das Datum der Zuweisung wird als erster Gültigkeitstag gesetzt.
Vererbung über dynamische Rolle	nur unbefristet Das Datum der Zuweisung wird als erster Gültigkeitstag gesetzt.
Vererbung über Systemrolle	nur unbefristet Das Datum der Zuweisung wird als erster Gültigkeitstag gesetzt.

Die Berechnung der effektiven Zuweisung wird über einen Zeitplan gesteuert.

- **Aktiv von (effektiv)**: kleinster erster Gültigkeitstag aus allen Zuweisungen
- **Aktiv bis (effektiv)**: größter letzter Gültigkeitstag aus allen befristeten Zuweisungen

  Wenn es eine unbefristete Zuweisung gibt, bleibt **Aktiv bis (effektiv)** leer.

Detaillierte Informationen zum Thema

- Zuweisen von E-Business Suite Berechtigungen an Benutzerkonten im One Identity Manager auf Seite 106

Verwandte Themen

- Ungültige Berechtigungszuweisungen auf Seite 122

Wirksamkeit von Berechtigungszuweisungen

Bei der Zuweisung von E-Business Suite Berechtigungen an Benutzerkonten kann es vorkommen, dass eine Person zwei oder mehr Berechtigungen erhält, die in dieser Kombination nicht auftreten dürfen. Um das zu verhindern, geben Sie die sich ausschließenden Berechtigungen bekannt. Dabei legen Sie für zwei Berechtigungen fest, welche der beiden Berechtigungen an Benutzerkonten wirksam werden soll, wenn beide zugewiesen sind.

Die Zuweisung einer ausgeschlossenen Berechtigungen 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 Berechtigungen kann nicht definiert werden. Das heißt, die Festlegung "Berechtigung A schließt Berechtigung B aus" UND "Berechtigung B schließt Berechtigung A aus" ist nicht zulässig.
- Für eine Berechtigung muss jede auszuschließende Berechtigung einzeln bekannt gegeben werden. Ausschlussdefinitionen werden nicht vererbt.

Die Wirksamkeit der Zuweisungen wird in der Tabelle EBSUserInResp über die Spalten ValidTo und XOrigin und in der Tabelle BaseTreeHasEBSResp über die Spalte XIsInEffect abgebildet.

Beispiel für die Wirksamkeit von Berechtigungen

- In einem E-Business Suite System sind die Berechtigungen A, B und C definiert.
- Berechtigung A wird über die Abteilung "Marketing", Berechtigung B über die Abteilung "Finanzen" und Berechtigung C wird über die Geschäftsrolle "Kontrollgruppe" zugewiesen.

Clara Harris hat ein Benutzerkonto in diesem System. 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 A, B und C.

Durch geeignete Maßnahmen soll verhindert werden, dass eine Person gleichzeitig die Berechtigungen A und B erhält. Das heißt, die Berechtigungen A und B schließen sich aus. Ein Benutzer, der die Berechtigung C besitzt, darf ebenfalls nicht gleichzeitig die Berechtigung B besitzen. Das heißt, die Berechtigungen B und C schließen sich aus.

Tabelle 30: Festlegen der ausgeschlossenen Berechtigungen (Tabelle `EBSRespExclusion`)

Wirksame Berechtigung	Ausgeschlossene Berechtigung
Berechtigung A	
Berechtigung B	Berechtigung A
Berechtigung C	Berechtigung B

Tabelle 31: Wirksame Zuweisungen

Person	Mitglied in Rolle	Wirksame Berechtigung
Ben King	Marketing	Berechtigung A
Jan Bloggs	Marketing, Finanzen	Berechtigung B
Clara Harris	Marketing, Finanzen, Kontrollgruppe	Berechtigung C
Jenny Basset	Marketing, Kontrollgruppe	Berechtigung A Berechtigung C

Für Clara Harris ist nur die Zuweisung der Berechtigung C wirksam und wird ins Zielsystem publiziert. Verlässt Clara Harris die Geschäftsrolle "Kontrollgruppe" zu einem späteren Zeitpunkt, wird die Berechtigung B wirksam.

Für Jenny Basset sind die Berechtigungen A und C wirksam, da zwischen beiden Berechtigungen kein Ausschluss definiert wurde. Soll das verhindert werden, definieren Sie einen weiteren Ausschluss für die Berechtigung C.

Tabelle 32: Ausgeschlossene Berechtigungen und wirksame Zuweisungen

Person	Mitglied in Rolle	Zugewiesene Berechtigung	Ausgeschlossene Berechtigung	Wirksame Berechtigung
Jenny Basset	Marketing	Berechtigung A		Berechtigung C
	Kontrollgruppe	Berechtigung C	Berechtigung B Berechtigung A	

Voraussetzungen

- Der Konfigurationsparameter **QER | Structures | Inherite | GroupExclusion** ist aktiviert.
- Sich ausschließende Berechtigungen gehören zum selben E-Business Suite System.

Um Berechtigungen auszuschließen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Berechtigungen**.
2. Wählen Sie in der Ergebnisliste eine Berechtigung.
3. Wählen Sie die Aufgabe **E-Business Suite Berechtigungen ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungen zu, die sich mit der gewählten Berechtigung ausschließen.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Berechtigungen, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Ungültige Berechtigungszuweisungen auf Seite 122

Vererbung von E-Business Suite Berechtigungen anhand von Kategorien

Im One Identity Manager können Berechtigungen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Berechtigungen 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 Berechtigungen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 31**.

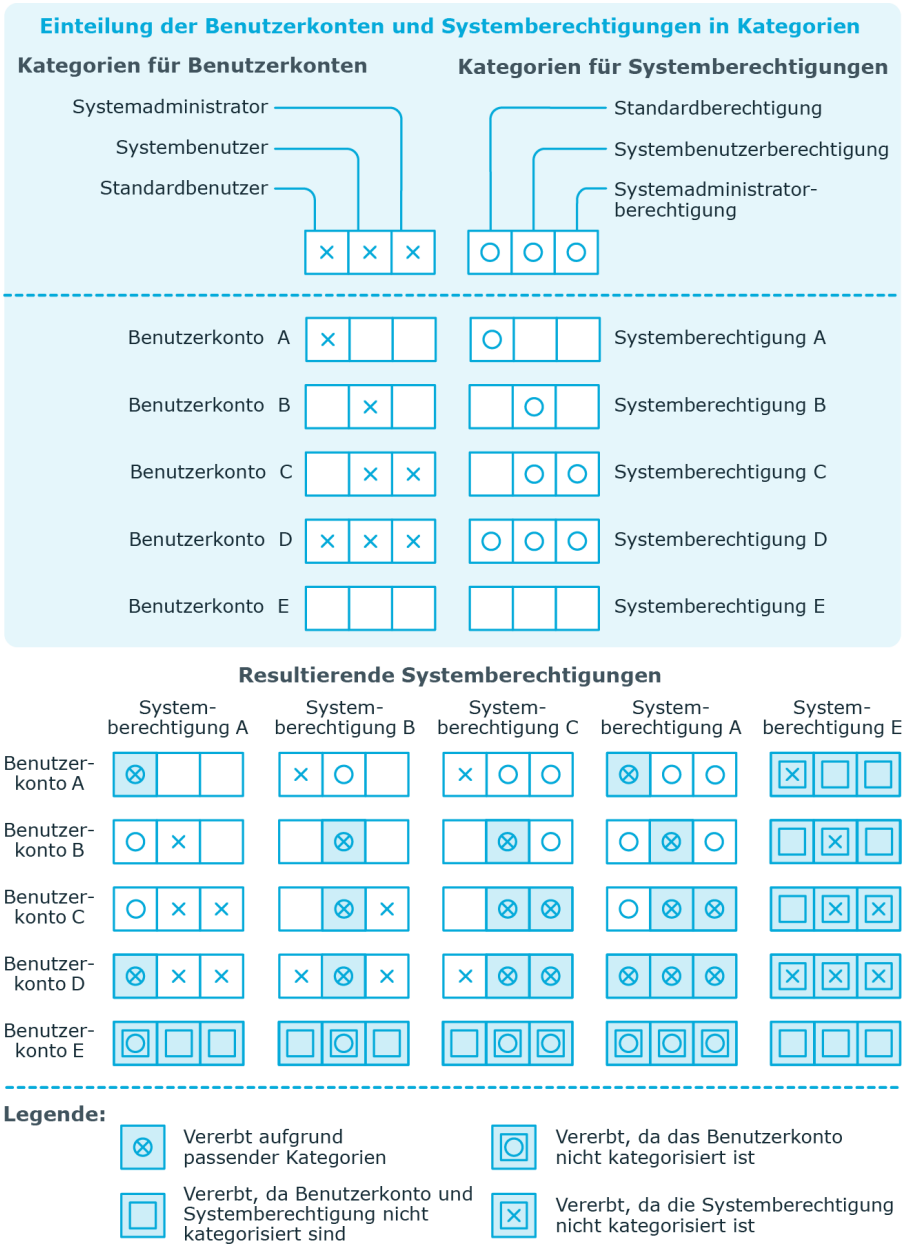
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Berechtigung kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Berechtigung überein, wird die Berechtigung an das Benutzerkonto vererbt. Ist die Berechtigung oder das Benutzerkonto nicht in Kategorien eingestuft, dann wird die Berechtigung ebenfalls an das Benutzerkonto vererbt.

HINWEIS: Die Vererbung über Kategorien wird nur bei der indirekten Zuweisung von Berechtigungen über hierarchische Rollen berücksichtigt. Bei der direkten Zuweisung von Berechtigungen an Benutzerkonten werden die Kategorien nicht berücksichtigt.

Tabelle 33: Beispiele für Kategorien

Kategorieposition	Kategorien für Benutzerkonten	Kategorien für Berechtigungen
1	Standardbenutzer	Standardberechtigung
2	Systembenutzer	Systembenutzerberechtigung
3	Systemadministrator	Systemadministratorberechtigung

Abbildung 2: Beispiel für die Vererbung über Kategorien



Um die Vererbung über Kategorien zu nutzen

- Definieren Sie am E-Business Suite System die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Berechtigungen über ihre Stammdaten zu.

Verwandte Themen

- Kategorien für die Vererbung von E-Business Suite Berechtigungen definieren auf Seite 127
- Allgemeine Stammdaten für E-Business Suite Benutzerkonten auf Seite 129
- Allgemeine Stammdaten für E-Business Suite Berechtigungen auf Seite 138

Ungültige Berechtigungszuweisungen

Berechtigungszuweisungen können nicht gelöscht werden. Durch verschiedene Vererbungsprozesse im One Identity Manager kann es jedoch passieren, dass eine Berechtigungszuweisung ungültig wird. Folgende Vorgänge können dafür verantwortlich sein:

- Abbestellen einer bestellten Berechtigungszuweisung oder Erreichen des Ablaufdatums einer Bestellung
- Entfernen einer direkten Berechtigungszuweisung im One Identity Manager
- Entfernen der Zuweisung einer Berechtigung zu hierarchischen oder dynamischen Rollen oder Systemrollen
- Entfernen der Mitgliedschaft eines Benutzerkontos in hierarchischen oder dynamischen Rollen
- Entfernen der Zuweisung eines Benutzerkontos zu Systemrollen
- Ausschließen von Berechtigungen
- Ändern der Kategorie, in die ein Benutzerkonto oder eine Berechtigung eingeordnet ist
- Deaktivieren/Löschen/Sicherheitsgefährdung von Personen und Behandlung der Benutzerkonten über eine Kontendefinition

  Für Benutzerkonten mit dem Automatisierungsgrad **Full managed** ist an der Kontendefinition geregelt, wie Berechtigungszuweisungen behandelt werden sollen, wenn die Person als sicherheitsgefährdend eingestuft, deaktiviert oder zum Löschen markiert wird. Wenn die Berechtigungszuweisungen nicht beibehalten werden sollen, wird sie als ungültig gekennzeichnet.
- Deaktivieren von Benutzerkonten

  Wenn das Benutzerkonto über eine Kontendefinition verwaltet wird, ist an der Kontendefinition geregelt, wie Berechtigungszuweisungen behandelt werden sollen.

Wenn die Berechtigungszuweisungen nicht beibehalten werden sollen, werden sie als ungültig gekennzeichnet.

Für ungültige Berechtigungszuweisungen liegt der Gültigkeitszeitraum in der Vergangenheit. Handelt es sich um vererbte oder bestellte Zuweisungen oder wurde eine Berechtigungszuweisung im Manager entfernt, erhält `XOrigin` den Wert **16**.

Wenn die Ursache für die Ungültigkeit einer Berechtigungszuweisung behoben ist, werden der letzte Gültigkeitstag und `XOrigin` auf ihre ursprünglichen Werte zurückgesetzt.

Verwandte Themen

- Wirksamkeit von Berechtigungszuweisungen auf Seite 118
- Stammdaten von Automatisierungsgraden auf Seite 63
- Stammdaten von Kontendefinitionen auf Seite 59
- E-Business Suite Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 108
- E-Business Suite Berechtigungen an Geschäftsrollen zuweisen auf Seite 109
- E-Business Suite Berechtigungen in Systemrollen aufnehmen auf Seite 110
- Vererbung von E-Business Suite Berechtigungen anhand von Kategorien auf Seite 120

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 3: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 34: 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.

Abbilden von E-Business Suite Objekten im One Identity Manager

Mit dem One Identity Manager verwalten Sie alle Objekte der Oracle E-Business Suite, die für die Optimierung der Zugriffssteuerung im Zielsystem benötigt werden. Diese Objekte werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können im Manager angezeigt oder bearbeitet werden.

E-Business Suite Systeme

Ein E-Business Suite System stellt das Zielsystem der Synchronisation einer Oracle E-Business Suite im One Identity Manager dar. E-Business Suite Systeme werden benötigt, um Provisionierungsprozesse, die automatische Zuordnung von Personen zu Benutzerkonten und die Vererbung von Berechtigungen an Benutzerkonten innerhalb einer Oracle E-Business Suite zu konfigurieren.

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

Um ein System einzurichten

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Systeme**.
2. Wählen Sie in der Ergebnisliste das System. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Bearbeiten Sie die Stammdaten für das System.
4. Speichern Sie die Änderungen.

Allgemeine Stammdaten für E-Business Suite Systeme

Auf dem Tabreiter **Allgemein** erfassen Sie die folgenden Stammdaten.

Tabelle 35: Allgemeine Stammdaten eines E-Business Suite Systems

Eigenschaft	Beschreibung
Anzeigename	Name des Systems zur Anzeige in der Benutzeroberfläche.
Kontendefinition (initial)	Initiale Kontendefinition zur Erzeugung von Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für dieses System 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.
Zielsystemverantwortliche	Anwendungsrolle, in der die Zielsystemverantwortlichen des Systems festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte des Systems, dem sie zugeordnet sind. Jedem System können andere Zielsystemverantwortliche zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle aus, deren Mitglieder verantwortlich für die Administration dieses Systems sind. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.
Synchronisiert durch	Art der Synchronisation, über welche die Daten zwischen dem System und dem One Identity Manager ausgetauscht werden. Sobald Objekte für dieses System im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden. Beim Erstellen eines Systems mit dem Synchronization Editor wird **One Identity Manager** verwendet.

Tabelle 36: Zulässige Werte

Wert	Synchronisation durch	Provisionierung durch
One Identity Manager	Oracle E-Business Suite Konnektor	Oracle E-Business Suite Konnektor
Keine Synchronisation	keine	keine

HINWEIS: Wenn Sie **Keine Synchronisation** festlegen,

Eigenschaft	Beschreibung
	definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.
Definierter Name	Eindeutiger Name für das System in X509-Syntax.

Verwandte Themen

- Kontendefinitionen an Zielsysteme zuweisen auf Seite 73
- Einrichten von Kontendefinitionen auf Seite 58
- Automatische Zuordnung von Personen zu E-Business Suite Benutzerkonten auf Seite 76
- Zielsystemverantwortliche auf Seite 161

Kategorien für die Vererbung von E-Business Suite Berechtigungen definieren

Im One Identity Manager können Berechtigungen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Berechtigungen 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 Berechtigungen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 31**.

Um Kategorien zu definieren

1. Wählen Sie im Manager in der Kategorie **Oracle E-Business Suite | Systeme** das System.
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 Berechtigungen in der verwendeten Anmeldesprache ein.
7. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Vererbung von E-Business Suite Berechtigungen anhand von Kategorien auf Seite 120

Synchronisationsprojekt bearbeiten

Synchronisationsprojekte, in denen ein System 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 im Manager die Kategorie **Oracle E-Business Suite | Systeme**.
2. Wählen Sie in der Ergebnisliste das System.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten**.

Verwandte Themen

- Anpassen einer Synchronisationskonfiguration auf Seite 29

E-Business Suite Benutzerkonten

Mit dem One Identity Manager verwalten Sie die Benutzerkonten einer Oracle E-Business Suite. Ein Benutzer kann sich mit seinem E-Business Suite Benutzerkonto an der Oracle E-Business Suite anmelden. Er verfügt dabei über alle Zuständigkeiten und Sicherheitsgruppen, die dem Benutzerkonto zugewiesen sind. Darüber hinaus können Verbindungen von Benutzerkonten zu Personen, die in der Oracle E-Business Suite verwaltet werden, abgebildet werden. Personendaten der Oracle E-Business Suite können mit der One Identity Manager-Datenbank synchronisiert und mit den Benutzerkonten verbunden werden.

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 E-Business Suite Benutzerkonto besitzen und über die Zuordnung zu einer primären Abteilung, einem primären Standort oder einer primären Kostenstelle ihre IT Betriebsdaten erhalten.

Verwandte Themen

- Managen von E-Business Suite Benutzerkonten und Personen auf Seite 57
- Einrichten von Kontendefinitionen auf Seite 58
- Standardprojektvorlagen für die Synchronisation einer Oracle E-Business Suite auf Seite 167
- Stammdaten für E-Business Suite Benutzerkonten erfassen auf Seite 129

Stammdaten für E-Business Suite Benutzerkonten erfassen

Um ein Benutzerkonto zu erstellen

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | 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 **Oracle E-Business Suite | 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.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für E-Business Suite Benutzerkonten auf Seite 129
- Anmeldedaten für E-Business Suite Benutzerkonten auf Seite 133

Allgemeine Stammdaten für E-Business Suite Benutzerkonten

Auf dem Tabreiter **Allgemein** erfassen Sie die folgenden Stammdaten.

Tabelle 37: Allgemeine Stammdaten eines 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** 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. 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.
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.
Benutzername	Bezeichnung des Benutzerkontos. Wenn Sie eine Kontendefinition zugeordnet haben, wird dieses Eingabefeld, abhängig vom Automatisierungsgrad, automatisch ausgefüllt.
Anzeigename	Anzeigename des Benutzerkontos. Wenn Sie eine Kontendefinition zugeordnet haben, wird dieses Eingabefeld, abhängig vom Automatisierungsgrad, automatisch ausgefüllt.
Definierter Name	Definierter Name des Benutzerkontos. Er wird per Bildungsregel

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td></td><td>aus dem Benutzernamen und dem definierten Namen des E-Business Suite Systems gebildet.</td></tr>
<tr><td>E-Mail-Adresse</td><td>E-Mail-Adresse des Benutzerkontos. Wenn Sie eine Kontendefinition zugeordnet haben, wird dieses Eingabefeld, abhängig vom Automatisierungsgrad, automatisch ausgefüllt.</td></tr>
<tr><td>Fax</td><td>Faxnummer des Benutzerkontos. Wenn Sie eine Kontendefinition zugeordnet haben, wird dieses Eingabefeld, abhängig vom Automatisierungsgrad, automatisch ausgefüllt.</td></tr>
<tr><td>Status</td><td>Status des Benutzerkontos. Der Status wird über eine Bildungsregel gesetzt. Der Wert ist abhängig vom Gültigkeitszeitraum des Benutzerkontos (Aktiv von (Datum), Aktiv bis (Datum)).

<table><tr><th>Status</th><th>Bedeutung</th></tr><tr><td>ACTIVE</td><td>Das aktuelle Datum liegt innerhalb des Gültigkeitszeitraums.</td></tr><tr><td>INACTIVE</td><td>• Das Aktiv-von-Datum ist noch nicht erreicht oder das Aktiv-bis-Datum liegt in der Vergangenheit.
• Das Benutzerkonto wurde gelöscht.</td></tr></table></td></tr>
<tr><td>Aktiv von (Datum)</td><td>Erstes Gültigkeitsdatum des Benutzerkontos. Wenn Sie eine Kontendefinition zugeordnet haben, wird dieses Eingabefeld, abhängig vom Automatisierungsgrad, automatisch ausgefüllt. Die Bildungsregel wirkt nur, wenn das Benutzerkonto neu angelegt wird.</td></tr>
<tr><td>Aktiv bis (Datum)</td><td>Letztes Gültigkeitsdatum des Benutzerkontos. Wenn Sie eine Kontendefinition zugeordnet haben, wird dieses Eingabefeld, abhängig vom Automatisierungsgrad, automatisch ausgefüllt.</td></tr>
<tr><td>E-Business Suite System</td><td>E-Business Suite System, in dem das Benutzerkonto angelegt werden soll.</td></tr>
<tr><td>Kunde</td><td>Verweis auf eine Person, die als Kunde geführt ist.

Es können nur Personen aus der Datenquelle E-Business Suite AR zugeordnet werden (<code>Person.ImportSource='EBSOIM'</code>).</td></tr>
<tr><td>HR Person</td><td>Verweis auf eine Person im Human Resources Modul der Oracle E-Business Suite.

Es können nur Personen aus der Datenquelle E-Business Suite HR zugeordnet werden (<code>Person.ImportSource='EBSHR'</code>).</td></tr>
</table>

Eigenschaft	Beschreibung
Beteiligter	Verweis auf eine Person, die als Beteiligter geführt ist. Es kann eine Person mit der Datenquelle **E-Business Suite AR** zugeordnet sein (`Person.ImportSource='EBSOIM'`). Die Zuordnung kann im One Identity Manager nicht bearbeitet werden.
Lieferant	Verweis auf eine Person, die als Lieferant oder Kontakt geführt ist. Es können nur Personen aus der Datenquelle **E-Business Suite AP** zugeordnet werden (`Person.ImportSource='EBSCRM'`).
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten Berechtigungen. 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 E-Business Suite Berechtigungen an das Benutzerkonto. Berechtigungen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Berechtigungen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
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.
Berechtigungen	Angabe, ob das Benutzerkonto E-Business Suite Berechtigungen

Eigenschaft	Beschreibung
erbbar	über die Person erben darf. Ist die Option aktiviert, werden Berechtigungen über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt. 1. Beispiel: Eine Person mit einem E-Business Suite Benutzerkonto ist Mitglied einer Abteilung. Dieser Abteilung ist eine E-Business Suite Berechtigung zugewiesen. Wenn die Option aktiviert ist, erbt das Benutzerkonto diese Berechtigung. 2. Beispiel: Eine Person mit einem E-Business Suite Benutzerkonto bestellt eine G Suite Berechtigung im IT Shop. Die Bestellung wird genehmigt und zugewiesen. Das Benutzerkonto erbt diese Berechtigung nur, wenn die Option aktiviert ist.
Benutzerkonto ist deaktiviert	Angabe, ob das Benutzerkonto für die Anmeldung am E-Business Suite System gesperrt ist. Per Bildungsregel wird der Status des Benutzerkontos übernommen. Um das Benutzerkonto zu deaktivieren, bearbeiten Sie das letzte Gültigkeitsdatum des Benutzerkontos.

Verwandte Themen

- Managen von E-Business Suite Benutzerkonten und Personen auf Seite 57
- Einrichten von Kontendefinitionen auf Seite 58
- Automatische Zuordnung von Personen zu E-Business Suite Benutzerkonten auf Seite 76
- Vererbung von E-Business Suite Berechtigungen anhand von Kategorien auf Seite 120
- E-Business Suite Benutzerkonten deaktivieren auf Seite 136
- Verbinden von E-Business Suite Benutzerkonten mit importierten Personen auf Seite 82
- Unterstützte Typen von Benutzerkonten auf Seite 85
- Nutzungsberechtigte Personen an ein Benutzerkonto mit Gruppenidentität zuweisen auf Seite 90

Anmeldedaten für E-Business Suite Benutzerkonten

Auf dem Tabreiter **Anmeldung** vergeben Sie das Kennwort für die Anmeldung an der Oracle E-Business Suite. Nach dem Speichern des Benutzerkontos kann das Kennwort über den One Identity Manager nicht mehr geändert werden.

Tabelle 38: Anmeldedaten eines Benutzerkontos

Eigenschaft	Beschreibung
Letzte Anmeldung	Datum der letzten Anmeldung.
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. Das Kennwort wird nach dem Publizieren in das Zielsystem aus der Datenbank gelöscht. 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.
Bestätigung	Kennwortwiederholung.
Anmeldevorgänge (verbleibend)	Anzahl der möglichen Anmeldevorgänge, bis das Kennwort abläuft.
Letzte Kennwortänderung	Datum der letzten Kennwortänderung.
Anmeldevorgänge	Anzahl zulässiger Anmeldevorgänge.
Tage	Gültigkeitszeitraum für das Kennwort.

Verwandte Themen

- Initiales Kennwort für neue E-Business Suite Benutzerkonten auf Seite 102

Zusätzliche Aufgaben zur Verwaltung von E-Business Suite Benutzerkonten

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

Aufgabe	Thema
Überblick über das E-Business Suite Benutzerkonto	Überblick über ein E-Business Suite Benutzerkonto auf Seite 135
Berechtigungen zuweisen	E-Business Suite Berechtigungen direkt an ein Benut-

Aufgabe	Thema
	zerkonto zuweisen auf Seite 114
Zusatzeigenschaften zuweisen	Zusatzeigenschaften an ein E-Business Suite Benutzerkonto zuweisen auf Seite 135
Personen mit Nutzungsberechtigungen zuzuweisen	Nutzungsberechtigte Personen an ein Benutzerkonto mit Gruppenidentität zuweisen auf Seite 90

Überblick über ein E-Business Suite Benutzerkonto

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das E-Business Suite Benutzerkonto**.

TIPP: Auf dem Überblicksformular können Sie mit einem Mausklick auf ein zugewiesenes Sicherheitsattribut das Stammdatenformular der Zuweisung öffnen. Hier sehen Sie den Wert, mit dem diese Zuweisung modifiziert ist.

Zusatzeigenschaften an ein E-Business Suite Benutzerkonto 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 **Oracle E-Business Suite | 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.

Ausführliche Informationen über Zusatzeigenschaften finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

E-Business Suite Benutzerkonten deaktivieren

Wie Sie Benutzerkonten deaktivieren, 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 deaktiviert, 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. Für Benutzerkonten mit einem anderen Automatisierungsgrad konfigurieren Sie das gewünschte Verhalten an der Bildungsregel der Spalte `EBSUser.EndDate`.

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 deaktiviert, 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 deaktiviert, wenn die Person zeitweilig oder dauerhaft deaktiviert wird.
- Ist der Konfigurationsparameter deaktiviert, haben die Eigenschaften der Person keinen Einfluss auf die verbundenen Benutzerkonten.

Um das Benutzerkonto bei deaktiviertem Konfigurationsparameter zu deaktivieren

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Setzen Sie auf dem Tabreiter **Allgemein** im Eingabefeld **Aktiv bis (Datum)** das aktuelle Datum.

   Der Status des Benutzerkontos wird auf **INACTIVE** gesetzt.
5. Speichern Sie die Änderungen.

Szenario:

- Benutzerkonten sind nicht mit Personen verbunden.

Um ein Benutzerkonto zu deaktivieren, das nicht mit einer Person verbunden ist

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Setzen Sie auf dem Tabreiter **Allgemein** im Eingabefeld **Aktiv bis (Datum)** das aktuelle Datum.

   Der Status des Benutzerkontos wird auf **INACTIVE** gesetzt.
5. Speichern Sie die Änderungen.

Um ein Benutzerkonto zu aktivieren

- Löschen Sie das letzte Gültigkeitsdatum im Eingabefeld **Aktiv bis (Datum)**.

Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Einrichten von Kontendefinitionen auf Seite 58
- Automatisierungsgrade erstellen auf Seite 61
- E-Business Suite Benutzerkonten löschen auf Seite 137

E-Business Suite Benutzerkonten löschen

E-Business Suite Benutzerkonten können im One Identity Manager nicht physisch gelöscht werden. Wenn ein Benutzerkonto über die Ergebnisliste oder über die Menüleiste gelöscht wird, wird das Benutzerkonto deaktiviert. Es bleibt physisch bestehen. Nach Bestätigung der Sicherheitsabfrage wird der Status des Benutzerkontos auf **INACTIVE** gesetzt. Das aktuelle Datum wird als letzter Gültigkeitstag am Benutzerkonto hinterlegt (**Aktiv bis (Datum)**).

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, deaktiviert.

Verwandte Themen

- E-Business Suite Benutzerkonten deaktivieren auf Seite 136

E-Business Suite Berechtigungen

E-Business Suite Benutzerkonten erhalten ihre Berechtigungen auf die Objekte einer Oracle E-Business Suite über Zuständigkeiten. Dabei können Zuständigkeiten nicht direkt an die Benutzerkonten zugewiesen werden, sondern werden über Sicherheitsgruppen vererbt. Berechtigungen in der Oracle E-Business Suite sind durch die Kombination aus Zuständigkeiten und Sicherheitsgruppen charakterisiert. Diese Kombinationen werden in der One Identity Manager-Datenbank als E-Business Suite Berechtigungen abgebildet.

Stammdaten für E-Business Suite Berechtigungen erfassen

Um die Stammdaten einer Berechtigung zu bearbeiten

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Berechtigungen**.
2. Um eine Berechtigung zu bearbeiten, wählen Sie in der Ergebnisliste die Berechtigung und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

   Um eine neue Berechtigung zu erstellen, klicken Sie in der Ergebnisliste .

   Das Stammdatenformular für eine E-Business Suite Berechtigung wird geöffnet.
3. Bearbeiten Sie die Stammdaten der Berechtigung.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für E-Business Suite Berechtigungen auf Seite 138

Allgemeine Stammdaten für E-Business Suite Berechtigungen

Für eine E-Business Suite Berechtigung bearbeiten Sie die folgenden Stammdaten.

Tabelle 39: Allgemeine Stammdaten einer Berechtigung

Eigenschaft	Beschreibung
E-Business Suite Zuständigkeit	Zuständigkeit, für welche die Berechtigung erstellt werden soll. Die Zuständigkeit muss zum selben E-Business Suite System gehören, wie die Sicherheitsgruppe.
Sicherheitsgruppe	Sicherheitsgruppe, für welche die Berechtigung erstellt werden soll. Die Sicherheitsgruppe muss zum selben E-Business Suite System gehören, wie die Zuständigkeit.
Anzeigename	Anzeigename der Berechtigung.
Kategorie	Kategorien für die Vererbung von Berechtigungen an Benutzerkonten. Berechtigungen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Berechtigungen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Berechtigung an Benutzerkonten. Stellen Sie einen Wert zwischen **0** und **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Leistungsposition	Angabe einer Leistungsposition, um die Berechtigung über den IT Shop zu bestellen.
IT Shop	Angabe, ob die Berechtigung über den IT Shop bestellbar ist. Die Berechtigung kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Berechtigung kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Berechtigung ausschließlich über den IT Shop bestellbar ist. Die Berechtigung kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Berechtigung an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.

Verwandte Themen

- Vererbung von E-Business Suite Berechtigungen anhand von Kategorien auf Seite 120
- E-Business Suite Berechtigungen in den IT Shop aufnehmen auf Seite 110

Zusätzliche Aufgaben zur Verwaltung von E-Business Suite Berechtigungen

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

Aufgabe	Thema
Überblick über die E-Business Suite Berechtigung	Überblick über eine E-Business Suite Berechtigung auf Seite 140
Benutzerkonten zuweisen	E-Business Suite Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 112
Zusatzeigenschaften zuweisen	Zusatzeigenschaften an eine E-Business Suite Berechtigung zuweisen auf Seite 140
E-Business Suite Berechtigungen ausschließen	Wirksamkeit von Berechtigungszuweisungen auf Seite 118
Systemrollen zuweisen	E-Business Suite Berechtigungen in Systemrollen aufnehmen auf Seite 110
Geschäftsrollen zuweisen	E-Business Suite Berechtigungen an Geschäftsrollen zuweisen auf Seite 109
Organisationen zuweisen	E-Business Suite Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 108
In IT Shop aufnehmen	E-Business Suite Berechtigungen in den IT Shop aufnehmen auf Seite 110

Überblick über eine E-Business Suite Berechtigung

Um einen Überblick über eine Berechtigung zu erhalten

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Berechtigungen**.
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Überblick über die E-Business Suite Berechtigung**.

Zusatzeigenschaften an eine E-Business Suite Berechtigung 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 Berechtigung festzulegen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Berechtigungen**.
2. Wählen Sie in der Ergebnisliste die E-Business Suite Berechtigung.
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.

E-Business Suite Anwendungen

Auf E-Business Suite Anwendungen werden die in der Oracle E-Business Suite integrierten Anwendungen abgebildet. Anwendungen werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können nicht bearbeitet werden.

Um die Eigenschaften einer Anwendung anzuzeigen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Anwendungen**.
2. Wählen Sie in der Ergebnisliste die Anwendung.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Auf dem Überblicksformular werden die Beziehungen einer Anwendung zu E-Business Suite Gruppen und Zuständigkeiten dargestellt.

Um einen Überblick über eine Anwendung zu erhalten

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Anwendungen**.
2. Wählen Sie in der Ergebnisliste die Anwendung.
3. Wählen Sie die Aufgabe **Überblick über die E-Business Suite Anwendung**.

E-Business Suite Menüs

Ein wichtiger Teil der Zugriffssteuerung in der Oracle E-Business Suite ist die Verlinkung eines Benutzerkontos zu einem Menü. Menüs werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können nicht bearbeitet werden.

Um die Eigenschaften eines Menüs anzuzeigen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Menüs**.
2. Wählen Sie in der Ergebnisliste das Menü.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Menüs werden über E-Business Suite Zuständigkeiten an Benutzerkonten zugewiesen. Jede Zuständigkeit kann genau ein Menü referenzieren. Diese Beziehung wird auf dem Überblicksformular eines Menüs dargestellt.

Um einen Überblick über ein Menü zu erhalten

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Menüs**.
2. Wählen Sie in der Ergebnisliste das Menü.
3. Wählen Sie die Aufgabe **Überblick über das E-Business Suite Menü**.

E-Business Suite Datengruppen

Über E-Business Suite Datengruppen wird der Zugriff von Benutzerkonten auf Tabellen im Datenbestand der Oracle E-Business Suite gesteuert. Datengruppen definieren, welche Tabellen zu einer E-Business Suite Anwendung gehören. Über die Zuordnung zu E-Business Suite Zuständigkeiten erhalten Benutzerkonten ihre Berechtigungen auf diese Tabellen. Datengruppen werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können nicht bearbeitet werden.

Um die Eigenschaften einer Datengruppe anzuzeigen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Datengruppen**.
2. Wählen Sie in der Ergebnisliste die Datengruppe.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Um einen Überblick über eine Datengruppe zu erhalten

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Datengruppen**.
2. Wählen Sie in der Ergebnisliste die Datengruppe.
3. Wählen Sie die Aufgabe **Überblick über die E-Business Suite Datengruppe**.

E-Business Suite Datengruppeneinheiten

In E-Business Suite Datengruppeneinheiten sind Datengruppen den E-Business Suite Anwendungen zugeordnet. Damit können die für eine Anwendung zugelassenen Datengruppen an E-Business Suite Zuständigkeiten zugewiesen werden. Datengruppeneinheiten werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Die Zuordnungen können nicht bearbeitet werden.

Um die Eigenschaften einer Datengruppeneinheit anzuzeigen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Anwendungen | <Anwendung> | Datengruppeneinheiten**.
2. Wählen Sie in der Ergebnisliste die Datengruppeneinheit.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Um einen Überblick über eine Datengruppeneinheit zu erhalten

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Anwendungen | <Anwendung> | Datengruppeneinheiten**.
2. Wählen Sie in der Ergebnisliste die Datengruppeneinheit.
3. Wählen Sie die Aufgabe **Überblick über die E-Business Suite Datengruppeneinheit**.

E-Business Suite Prozessgruppen

Über E-Business Suite Prozessgruppen werden Berechtigungen zum Ausführen von Programmen und Funktionen vergeben. Prozessgruppen sind E-Business Suite Anwendungen zugeordnet. Sie werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können nicht bearbeitet werden.

Um die Eigenschaften einer Prozessgruppe anzuzeigen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Anwendungen | <Anwendung> | Prozessgruppen**.
2. Wählen Sie in der Ergebnisliste die Prozessgruppe.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Um einen Überblick über eine Prozessgruppe zu erhalten

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Anwendungen | <Anwendung> | Prozessgruppen**.
2. Wählen Sie in der Ergebnisliste die Prozessgruppe.
3. Wählen Sie die Aufgabe **Überblick über die E-Business Suite Prozessgruppe**.

E-Business Suite Sicherheitsgruppen

Über E-Business Suite Sicherheitsgruppen werden die Zuständigkeiten von Benutzerkonten weiter eingeschränkt. Sicherheitsgruppen werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können nicht bearbeitet werden.

Um die Eigenschaften einer Sicherheitsgruppe anzuzeigen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Sicherheitsgruppen**.
2. Wählen Sie in der Ergebnisliste die Sicherheitsgruppe.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Um einen Überblick über eine Sicherheitsgruppe zu erhalten

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Sicherheitsgruppen**.
2. Wählen Sie in der Ergebnisliste die Sicherheitsgruppe.
3. Wählen Sie die Aufgabe **Überblick über die E-Business Suite Sicherheitsgruppe**.

E-Business Suite Attribute

E-Business Suite Attribute schränken die Zuständigkeiten von Benutzerkonten weiter ein. Sie können zu diesem Zweck sowohl an Benutzerkonten als auch an Zuständigkeiten zugewiesen sein. Attribute werden je E-Business Suite Anwendung definiert. Sie werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können nicht bearbeitet werden.

Um die Eigenschaften eines Attributs anzuzeigen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Anwendungen | <Anwendung> | Attribute**.

2. Wählen Sie in der Ergebnisliste das Attribut.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Attribute, die an Benutzerkonten oder Zuständigkeiten zugewiesen sind, werden als Sicherheitsattribute bezeichnet. Sie können durch zusätzliche Werte modifiziert sein. Diese Beziehungen werden auf dem Überblicksformular eines Attributs dargestellt.

Um einen Überblick über ein Attribut zu erhalten

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Anwendungen | <Anwendung> | Attribute**.
2. Wählen Sie in der Ergebnisliste das Attribut.
3. Wählen Sie die Aufgabe **Überblick über das E-Business Suite Attribut**.

Auf dem Überblicksformular eines Attributs können Sie mit einem Mausklick auf ein zugewiesenes Benutzerkonto oder eine zugewiesene Zuständigkeit das Stammdatenformular der Zuweisung öffnen. Hier sehen Sie den Wert, mit dem diese Zuweisung modifiziert ist.

E-Business Suite Zuständigkeiten

E-Business Suite Zuständigkeiten steuern die Zugriffsrechte eines Benutzerkontos in der Oracle E-Business Suite. Zuständigkeiten beziehen sich auf genau eine Version. E-Business Suite Zuständigkeiten werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können nicht bearbeitet werden.

E-Business Suite Attribute schränken die Zuständigkeiten weiter ein. Dafür können Listen von Sicherheitsattributen und Ausschlussattributen definiert sein. Untermenüs können explizit von der Zuordnung zu einer Zuständigkeit ausgeschlossen sein. Diese Beziehungen werden auf dem Überblicksformular dargestellt.

Stammdaten für E-Business Suite Zuständigkeiten anzeigen

Um die Eigenschaften einer Zuständigkeit anzuzeigen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Anwendungen | <Anwendung> | Zuständigkeiten**.
2. Wählen Sie in der Ergebnisliste die Zuständigkeit.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Um einen Überblick über eine Zuständigkeit zu erhalten

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Baumdarstellung | <E-Business Suite System> | Anwendungen | <Anwendung> | Zuständigkeiten**.
2. Wählen Sie in der Ergebnisliste die Zuständigkeit.
3. Wählen Sie die Aufgabe **Überblick über die E-Business Suite Zuständigkeit**.

Auf dem Überblicksformular einer Zuständigkeit können Sie mit einem Mausklick auf ein zugewiesenes Sicherheitsattribut das Stammdatenformular der Zuweisung öffnen. Hier sehen Sie den Wert, mit dem diese Zuweisung modifiziert ist.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für E-Business Suite Zuständigkeiten auf Seite 146

Allgemeine Stammdaten für E-Business Suite Zuständigkeiten

Für E-Business Suite Zuständigkeiten werden folgende Eigenschaften abgebildet.

Tabelle 40: Allgemeine Stammdaten einer Zuständigkeit

Eigenschaft	Beschreibung
Kennung	Eindeutige Kennung der Zuständigkeit in der E-Business Suite.
Zuständigkeitsschlüssel	Bezeichnung der Zuständigkeit. Der Zuständigkeitsschlüssel ist je Anwendung eindeutig.
Name der Zuständigkeit	Anzeigename der Zuständigkeit.
Gültig von (Datum)	Erstes Gültigkeitsdatum der Zuständigkeit.
Gültig bis (Datum)	Letztes Gültigkeitsdatum der Zuständigkeit. Wenn dieses Datum abgelaufen ist, ist die Zuständigkeit deaktiviert.
Beschreibung	Zusätzliche Informationen zur Zuständigkeit.
Sprache	Sprachcode der Sprache, in der die Zuständigkeit in der Oracle E-Business Suite hinterlegt ist.
Anwendung	Anwendung, in der die Zuständigkeit gültig ist.
Datengruppeneinheit	Datengruppeneinheit, für welche die Zuständigkeit gilt.
Menü	Menü, für das die Zuständigkeit gilt.

Eigenschaft	Beschreibung
Prozessgruppe	Prozessgruppe, für welche die Zuständigkeit gilt.
Version	Version, in der die Zuständigkeit verfügbar ist. Werte können sein: • AOL (Oracle Applications) • Web (Oracle Self-Service Web Applications) • Mobile (Oracle Mobile Applications) • Direct Access • None
Web-Host	IP-Adresse oder Name des Webservers.
Web-Agent	Name des Web-Agenten, der die Datenbank spezifiziert.
Terminalberechtigungen	Gibt an, ob Terminalberechtigungen für die Zuständigkeit zugelassen sind.

HR Personen

HR Personen sind alle Personen, die aus der Tabelle HR.PER_ALL_PEOPLE_F der Oracle E-Business Suite importiert wurden. Diese Personen können als HR Person an E-Business Suite Benutzerkonten zugeordnet werden. Zusätzlich werden die Manager der HR Personen importiert.

Um die Eigenschaften einer HR Person anzuzeigen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | HR Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   Auf dem Tabreiter **Sonstiges** wird die Eigenschaft **Datenquelle Import** mit dem Wert **E-Business Suite HR** angezeigt.
4. Wählen Sie die Aufgabe **Überblick über die Person**.

   Auf dem Überblicksformular werden die Benutzerkonten angezeigt, denen die Person als HR Person zugeordnet ist.

Die Stammdaten der importierten Personen können im One Identity Manager nur eingeschränkt bearbeitet werden, da die Oracle E-Business Suite für bestimmte Eigenschaften das Mastersystem ist.

Für die Bearbeitung gesperrte Personenstammdaten:

- Vorname
- Nachname

- Anrede
- Zweiter Vorname
- Geburtsname
- Geburtsdatum
- Eintrittsdatum
- Manager
- Primärer Standort

Alle übrigen Stammdaten können in gewohnter Weise gepflegt werden. Ausführliche Informationen über die Bearbeitung von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

HINWEIS: Personen, die aus der Oracle E-Business Suite importiert wurden, können im One Identity Manager nicht gelöscht werden.

Verwandte Themen

- Verbinden von E-Business Suite Benutzerkonten mit importierten Personen auf Seite 82
- Allgemeine Stammdaten für E-Business Suite Benutzerkonten auf Seite 129
- Synchronisationsprojekt für Personendaten erstellen auf Seite 26
- Projektvorlage für HR-Daten auf Seite 168

Lieferanten und Kontakte

Lieferanten und Kontakte sind alle Personen, die aus der Tabelle `AP.AP_SUPPLIER_CONTACTS` der Oracle E-Business Suite importiert wurden. Diese Personen können als Lieferant an E-Business Suite Benutzerkonten zugeordnet werden.

Um die Eigenschaften eines Lieferanten anzuzeigen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Lieferanten und Kontakte**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   Auf dem Tabreiter **Sonstiges** wird die Eigenschaft **Datenquelle Import** mit dem Wert **E-Business Suite AP** angezeigt.
4. Wählen Sie die Aufgabe **Überblick über die Person**.

   Auf dem Überblicksformular werden die Benutzerkonten angezeigt, denen die Person als Lieferant zugeordnet ist.

Die Stammdaten der importierten Personen können im One Identity Manager nur eingeschränkt bearbeitet werden, da die Oracle E-Business Suite für bestimmte Eigenschaften das Mastersystem ist.

Für die Bearbeitung gesperrte Personenstammdaten:

- Vorname
- Nachname
- Anrede
- Zweiter Vorname
- Titel
- Standard-E-Mail-Adresse
- Telefon

Alle übrigen Stammdaten können in gewohnter Weise gepflegt werden. Ausführliche Informationen über die Bearbeitung von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

HINWEIS: Personen, die aus der Oracle E-Business Suite importiert wurden, können im One Identity Manager nicht gelöscht werden.

Verwandte Themen

- Verbinden von E-Business Suite Benutzerkonten mit importierten Personen auf Seite 82
- Allgemeine Stammdaten für E-Business Suite Benutzerkonten auf Seite 129
- Synchronisationsprojekt für organisatorische Daten erstellen auf Seite 27
- Projektvorlage für CRM-Daten auf Seite 169

Beteiligte

Beteiligte sind alle Personen, die aus der Tabelle `AR.HZ_PARTIES` der Oracle E-Business Suite importiert wurden. Diese Personen können als Kunden an E-Business Suite Benutzerkonten zugeordnet werden. Die Zuordnung als Beteiligter kann nur durch die Synchronisation in die One Identity Manager-Datenbank eingelesen werden.

Um die Eigenschaften eines Beteiligten anzuzeigen

1. Wählen Sie die Kategorie **Oracle E-Business Suite | Beteiligte**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   Auf dem Tabreiter **Sonstiges** wird die Eigenschaft **Datenquelle Import** mit dem Wert **E-Business Suite AR** angezeigt.
4. Wählen Sie die Aufgabe **Überblick über die Person**.

   Auf dem Überblicksformular werden die Benutzerkonten angezeigt, denen die Person als Beteiligter oder Kunde zugeordnet ist.

Die Stammdaten der importierten Personen können im One Identity Manager nur eingeschränkt bearbeitet werden, da die Oracle E-Business Suite für bestimmte Eigenschaften das Mastersystem ist.

Für die Bearbeitung gesperrte Personenstammdaten:

- Vorname
- Nachname
- Anrede
- Ort
- Postleitzahl
- Straße
- Land
- Bundesland

Alle übrigen Stammdaten können in gewohnter Weise gepflegt werden. Ausführliche Informationen über die Bearbeitung von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

HINWEIS: Personen, die aus der Oracle E-Business Suite importiert wurden, können im One Identity Manager nicht gelöscht werden.

Verwandte Themen

- Verbinden von E-Business Suite Benutzerkonten mit importierten Personen auf Seite 82
- Allgemeine Stammdaten für E-Business Suite Benutzerkonten auf Seite 129
- Synchronisationsprojekt für organisatorische Daten erstellen auf Seite 27
- Projektvorlage für OIM-Daten auf Seite 169

Standorte

Bei der Synchronisation von Daten aus dem Human Resources Modul der Oracle E-Business Suite werden neben den Personendaten auch Standortdaten sowie die Zuordnungen von Personen zu Standorten eingelesen. Die Standorte werden mit der Datenquelle Import **E-Business Suite HR** abgebildet.

Um Standorte anzuzeigen, die aus dem Import von HR Daten stammen

- Wählen Sie die Kategorie **Organisationen | Standorte | Datenquelle | E-Business Suite HR**.

Die Stammdaten der importierten Standorte können im One Identity Manager nur eingeschränkt bearbeitet werden, da die Oracle E-Business Suite für bestimmte Eigenschaften das Mastersystem ist.

Für die Bearbeitung gesperrte Stammdaten:

- Standort
- Beschreibung
- Straße
- Ort
- Land

Alle übrigen Stammdaten können in gewohnter Weise gepflegt werden. Ausführliche Informationen über die Bearbeitung von Standorten finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

HINWEIS: Standorte, die aus der Oracle E-Business Suite importiert wurden, können im One Identity Manager nicht gelöscht werden.

Verwandte Themen

- Synchronisationsprojekt für Personendaten erstellen auf Seite 26
- Projektvorlage für HR-Daten auf Seite 168

Abteilungen

Bei der Synchronisation von Daten aus dem Human Resources Modul der Oracle E-Business Suite werden neben den Personendaten auch Abteilungen sowie die Zuordnungen von Personen zu Abteilungen eingelesen. Die Abteilungen werden mit der Datenquelle Import **E-Business Suite HR** abgebildet.

Um Abteilungen anzuzeigen, die aus dem Import von HR Daten stammen

- Wählen Sie im Manager die Kategorie **Organisationen | Abteilungen | Datenquelle | E-Business Suite HR**.

Ausführliche Informationen über die Bearbeitung von Abteilungen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

HINWEIS: Abteilungen, die aus der Oracle E-Business Suite importiert wurden, können im One Identity Manager nicht gelöscht werden.

Verwandte Themen

- Synchronisationsprojekt für Personendaten erstellen auf Seite 26
- Projektvorlage für HR-Daten auf Seite 168
- Synchronisation von Abteilungen konfigurieren auf Seite 34

Berichte über E-Business Suite Objekte

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 E-Business Suite Systeme stehen folgende Berichte zur Verfügung.

Tabelle 41: Berichte für das Zielsystem

Bericht	Beschreibung
Übersicht aller Zuweisungen (System)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die in dem ausgewählten System mindestens ein Benutzerkonto besitzen.
Übersicht aller Zuweisungen (Berechtigung)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, welche die ausgewählte Berechtigung besitzen.
E-Business Suite Benutzerkonten- und Berechtigungsverteilung	Der Bericht enthält eine Zusammenfassung zur Benutzerkonten- und Berechtigungsverteilung aller E-Business Suite Systeme. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager| Übersichten Zielsysteme**.
Ungenutzte Benutzerkonten anzeigen	Der Bericht enthält alle Benutzerkonten des ausgewählten Systems, die in den letzten Monaten nicht verwendet wurden. Der Bericht enthält die Gruppenmitgliedschaften und die Risikoeinschätzung. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager| Analyse Datenqualität**.
Abweichende Systemberechtigungen anzeigen	Der Bericht enthält alle Berechtigungen des ausgewählten Systems, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager| Analyse Datenqualität**.
Benutzerkonten mit einer überdurchschnittlichen Anzahl an Systemberechtigungen anzeigen	Der Bericht enthält alle Benutzerkonten des ausgewählten Systems, die eine überdurchschnittliche Anzahl an zugewiesenen Berechtigungen besitzen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager| Analyse Datenqualität**.
Unverbundene Benutzerkonten anzeigen	Der Bericht enthält alle unverbundenen Benutzerkonten des ausgewählten Systems einschließlich ihrer zugeordneten Berechtigungen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager| Analyse Datenqualität**.
Datenqualität der E-Business Suite Benutzerkonten	Der Bericht enthält verschiedenen Auswertungen zur Datenqualität der Benutzerkonten aller E-Business Suite Systeme. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager | Analyse Datenqualität**.

7

Behandeln von E-Business Suite Objekten im Web Portal

Der One Identity Manager bietet seinen Benutzern die Möglichkeit, verschiedene Aufgaben unkompliziert über ein Web Portal zu erledigen. Das Web Portal unterstützt die Administration einer Oracle E-Business Suite bei folgenden Aufgaben:

- Managen von Benutzerkonten und Personen

  Mit der Zuweisung einer Kontendefinition an ein IT Shop Regal kann die Kontendefinition von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Person, beispielsweise einen Manager, wird das Benutzerkonto angelegt.

- Managen von Berechtigungszuweisungen

  Mit der Zuweisung einer E-Business Suite Berechtigung an ein IT Shop Regal kann die Berechtigung von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Person wird die Berechtigung zugewiesen.

  Manager und Administratoren von Organisationen können im Web Portal E-Business Suite Berechtigungen an die Abteilungen, Kostenstellen oder Standorte zuweisen, für die sie verantwortlich sind. Die Berechtigungen werden an alle Personen vererbt, die Mitglied dieser Abteilungen, Kostenstellen oder Standorte sind.

  Wenn das Geschäftsrollenmodul vorhanden ist, können Manager und Administratoren von Geschäftsrollen im Web Portal E-Business Suite Berechtigungen an die Geschäftsrollen zuweisen, für die sie verantwortlich sind. Die Berechtigungen werden an alle Personen vererbt, die Mitglied dieser Geschäftsrollen sind.

  Wenn das Systemrollenmodul vorhanden ist, können Verantwortliche von Systemrollen im Web Portal E-Business Suite Berechtigungen an die Systemrollen zuweisen. Die Berechtigungen werden an alle Personen vererbt, denen diese Systemrollen zugewiesen sind.

- Attestierung

  Wenn das Modul Attestierung vorhanden ist, kann die Richtigkeit der Eigenschaften von Zielsystemobjekten und von Berechtigungszuweisungen regelmäßig oder auf Anfrage bescheinigt werden. Dafür werden im Manager Attestierungsrichtlinien

konfiguriert. Die Attestierer nutzen das Web Portal, um Attestierungsvorgänge zu entscheiden.

- Governance Administration

  Wenn das Modul Complianceregeln vorhanden ist, können Regeln definiert werden, die unzulässige Berechtigungszuweisungen identifizieren und deren Risiken bewerten. Die Regeln werden regelmäßig und bei Änderungen an den Objekten im One Identity Manager überprüft. Complianceregeln werden im Manager definiert. Verantwortliche Personen nutzen das Web Portal, um Regelverletzungen zu überprüfen, aufzulösen und Ausnahmegenehmigungen zu erteilen.

  Wenn das Modul Unternehmensrichtlinien vorhanden ist, können Unternehmensrichtlinien für die im One Identity Manager abgebildeten Zielsystemobjekte definiert und deren Risiken bewertet werden. Unternehmensrichtlinien werden im Manager definiert. Verantwortliche Personen nutzen das Web Portal, um Richtlinienverletzungen zu überprüfen und Ausnahmegenehmigungen zu erteilen.

- Risikobewertung

  Über den Risikoindex von E-Business Suite Berechtigungen kann das Risiko von Berechtigungszuweisungen für das Unternehmen bewertet werden. Dafür stellt der One Identity Manager Standard-Berechnungsvorschriften bereit. Im Web Portal können die Berechnungsvorschriften modifiziert werden.

- Berichte und Statistiken

  Das Web Portal stellt verschiedene Berichte und Statistiken über die Personen, Benutzerkonten, deren Berechtigungen und Risiken bereit.

Ausführliche Informationen zu den genannten Themen finden Sie unter Zuweisen von E-Business Suite Berechtigungen an Benutzerkonten im One Identity Manager auf Seite 106 und in folgenden Handbüchern:

- One Identity Manager Anwenderhandbuch für das Web Portal
- One Identity Manager Administrationshandbuch für Attestierungen
- One Identity Manager Administrationshandbuch für Complianceregeln
- One Identity Manager Administrationshandbuch für Unternehmensrichtlinien
- One Identity Manager Administrationshandbuch für Risikobewertungen

8

Basisdaten zur Konfiguration

Für die Verwaltung einer Oracle E-Business Suite im One Identity Manager sind folgende Basisdaten relevant.

- 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 58.

- 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 E-Business Suite Benutzerkonten auf Seite 91.

- 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 Ausstehende Objekte nachbearbeiten auf Seite 52.

- Server

  Für die Verarbeitung der Oracle E-Business Suite-spezifischen Prozesse im One Identity Manager muss der Synchronisationsserver mit seinen Serverfunktionen bekannt sein.

Weitere Informationen finden Sie unter Jobserver für E-Business Suite-spezifische Prozessverarbeitung auf Seite 156.

- Zielsystemverantwortliche

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

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

  Weitere Informationen finden Sie unter Zielsystemverantwortliche auf Seite 161.

Jobserver für E-Business Suite-spezifische Prozessverarbeitung

Für die Verarbeitung der Oracle E-Business Suite-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 **Oracle E-Business Suite | 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.

Verwandte Themen

- Systemanforderungen für den Synchronisationsserver auf Seite 17

E-Business Suite Jobserver bearbeiten

Um einen Jobserver und seine Funktionen zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Oracle E-Business Suite | 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

- Allgemeine Stammdaten für Jobserver auf Seite 157
- Festlegen der Serverfunktionen auf Seite 160

Allgemeine Stammdaten für Jobserver

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 42: Eigenschaften eines Jobservers

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

Eigenschaft	Bedeutung
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. 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.

Eigenschaft	Bedeutung
	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 | 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 160

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 43: Zulässige Serverfunktionen

Serverfunktion	Anmerkungen
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.
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.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
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.
Oracle E-Business Suite Konnektor	Server, auf dem der Oracle E-Business Suite Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem Oracle E-Business Suite aus.

Verwandte Themen

- Allgemeine Stammdaten für Jobserver auf Seite 157

Zielsystemverantwortliche

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

Wenn Sie die Bearbeitungsrechte der Zielsystemverantwortlichen auf einzelne Systeme 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 E-Business Suite Systeme 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 E-Business Suite Systemen zuweisen.

Tabelle 44: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Oracle E-Business Suite** 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.

Benutzer	Aufgaben
	• Bereiten Berechtigungen 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. • 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 | Oracle E-Business Suite**.
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 **Oracle E-Business Suite | 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 E-Business Suite Systeme festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **Oracle E-Business Suite | Systeme**.
3. Wählen Sie in der Ergebnisliste das System.
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 | Oracle E-Business Suite** 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, das System im One Identity Manager zu bearbeiten.

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer Oracle E-Business Suite auf Seite 9
- Allgemeine Stammdaten für E-Business Suite Systeme auf Seite 125

Anhang A

Benötigte Berechtigungen für die Synchronisation mit einer Oracle E-Business Suite

Der Oracle E-Business Suite Konnektor benötigt lesenden Zugriff auf mindestens folgende Datenbankobjekte in der anzubindenden Oracle Database.

Tabelle 45: Tabellen und Views mit Select-Berechtigungen

Tabellen	Views
• ak.ak_attributes_tl • ak.ak_excluded_items • ak.ak_resp_security_attr_values • ak.ak_web_user_sec_attr_values • applsys.fnd_application • applsys.fnd_application_tl • applsys.fnd_data_groups • applsys.fnd_data_group_units • applsys.fnd_languages • applsys.fnd_menus • applsys.fnd_menus_tl • applsys.fnd_profile_options • applsys.fnd_profile_option_values • applsys.fnd_request_groups • applsys.fnd_resp_functions • applsys.fnd_responsibility • applsys.fnd_responsibility_tl • applsys.fnd_security_groups	• ak.ak_attributes_tl# • ak.ak_excluded_items# • ak.ak_resp_security_attr_values# • ak.ak_web_user_sec_attr_values# • applsys.fnd_application# • applsys.fnd_application_tl# • applsys.fnd_data_groups# • applsys.fnd_data_group_units# • applsys.fnd_languages# • applsys.fnd_menus# • applsys.fnd_menus_tl# • applsys.fnd_request_groups# • applsys.fnd_responsibility# • applsys.fnd_responsibility_tl# • applsys.fnd_security_groups# • applsys.fnd_security_groups_tl# • applsys.fnd_user#

Tabellen	Views
• applsys.fnd_security_groups_tl • applsys.fnd_user • apps.fnd_user_resp_groups_all • apps.fnd_user_resp_groups_direct • apps.fnd_user_resp_groups_indirect • apps.fnd_usr_roles	

Tabelle 46: Tabellen mit Select-Berechtigungen für die Synchronisation von Personendaten

Tabellen	Views
• ap.ap_supplier_contacts • ar.hz_parties • hr.hr_all_organization_units • hr.hr_locations_all • hr.per_all_assignments_f • hr.per_all_people_f • hr.per_job_groups • hr.per_jobs • hr.per_org_structure_versions • hr.per_org_structure_elements • hr.per_roles • hr.per_sec_profile_assignments • hr.per_security_profiles	• hr.hr_all_organization_units# • hr.hr_locations_all# • hr.per_all_assignments_f# • hr.per_all_people_f# • hr.per_job_groups# • hr.per_jobs# • hr.per_org_structure_versions# • hr.per_org_structure_elements# • hr.per_sec_profile_assignments# • hr.per_security_profiles#

Tabelle 47: Tabellen mit Ausführungsberechtigungen für die Synchronisation von Personendaten

Tabellen
• hr.per_sec_profile_asg_api

Tabelle 48: Tabellen mit Select-Berechtigungen für Schematypen, die im Konnektorschema angelegt, aber nicht im Standard-Mapping enthalten sind

Tabellen	Views
• applsys.fnd_request_group_units • applsys.fnd_request_sets	• applsys.fnd_request_group_units# • applsys.fnd_request_sets#

Tabellen	Views
• applsys.fnd_request_sets_tl • applsys.fnd_user_preferences	• applsys.fnd_user_preferences#

Tabelle 49: Stored Procedures mit Ausführungsberechtigungen

Stored Procedures
• apps.fnd_user_pkg Damit werden Berechtigungen auf die folgenden Procedures erteilt. • apps.fnd_user_pkg.AddResp • apps.fnd_user_pkg.change_user_name • apps.fnd_user_pkg.changepassword • apps.fnd_user_pkg.CreateUser • apps.fnd_user_pkg.DelResp • apps.fnd_user_pkg.DisableUser • apps.fnd_user_pkg.UpdateUser • apps.fnd_user_pkg.user_synch

Anhang B

Standardprojektvorlagen für die Synchronisation einer Oracle E-Business Suite

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 Benutzerkonten und Berechtigungen auf Seite 167
- Projektvorlage für HR-Daten auf Seite 168
- Projektvorlage für CRM-Daten auf Seite 169
- Projektvorlage für OIM-Daten auf Seite 169

Projektvorlage für Benutzerkonten und Berechtigungen

Für die Synchronisation von Benutzerkonten und Berechtigungen einer Oracle E-Business Suite nutzen Sie die Projektvorlage **Oracle E-Business Suite Synchronisation**. Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 50: Abbildung der E-Business Suite-Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im Zielsystem	Tabelle im One Identity Manager Schema
ORA-Account	EBSUser
ORA-Application	EBSApplication
ORA-Attribute	EBSAttribute
ORA-Datagroup	EBSDataGroup
ORA-Datagroupunit	EBSDataGroupUnit
ORA-Language	EBSLanguage
ORA-Menu	EBSMenu
ORA-Requestgroup	EBSRequestGroup
ORA-RESP	EBSResp
ORA-Responsibility	EBSResponsibility
ORA-ResponsiExcludesAttribute	EBSResponsiExcludesAttribute
ORA-ResponsiExcludesMenu	EBSResponsiExcludesMenu
ORA-ResponsiHasAttribute	EBSResponsiHasAttribute
ORA-Securitygroup	EBSSecurityGroup
ORA-UserHasAttribute	EBSUserHasAttribute
UserInRespDirect	EBSUserInResp
UserInRespIndirect	EBSUserInResp

Projektvorlage für HR-Daten

Für die Synchronisation von HR Personendaten aus dem Human-Resources-Modul einer Oracle E-Business Suite nutzen Sie die Projektvorlage **Oracle E-Business Suite HR-Daten**. Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 51: Abbildung der E-Business Suite-Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im Zielsystem	Tabelle im One Identity Manager Schema
HRPerson	Person
HRPersonManager	Person

Schematyp im Zielsystem	Tabelle im One Identity Manager Schema
HRLocations	Locality
HRPersonSecondaryLocation	PersonInLocality
HRPersonPrimaryLocation	Person
HROrganization	Department
HRPersonInOrganization	PersonInDepartment

Projektvorlage für CRM-Daten

Für die Synchronisation von Lieferanten-Kontaktdaten einer Oracle E-Business Suite nutzen Sie die Projektvorlage **Oracle E-Business Suite CRM-Daten**. Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 52: Abbildung der E-Business Suite-Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im Zielsystem	Tabelle im One Identity Manager Schema
APSupplierContacts	Person

Projektvorlage für OIM-Daten

Für die Synchronisation von Beteiligten-Personendaten einer Oracle E-Business Suite nutzen Sie die Projektvorlage **Oracle E-Business Suite OIM-Daten**. Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 53: Abbildung der E-Business Suite-Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im Zielsystem	Tabelle im One Identity Manager Schema
HZParty	Person

Anhang C

Verarbeitung von Systemobjekten

Folgende Tabelle beschreibt die zulässigen Verarbeitungsmethoden für die Schematypen der Oracle E-Business Suite und benennt notwendige Einschränkungen bei der Verarbeitung der Systemobjekte.

Tabelle 54: Zulässige Verarbeitungsmethoden für Schematypen

Schematyp	Lesen	Einfügen	Löschen	Aktualisieren
Anwendung (ORA-Application)	Ja	Nein	Nein	Nein
Attribut (ORA-Attribute)	Ja	Nein	Nein	Nein
Sprache (ORA-Language)	Ja	Nein	Nein	Nein
Menü (ORA-Menu)	Ja	Nein	Nein	Nein
Benutzerkonto (ORA-Account)	Ja	Ja	Nein	Ja
Datengruppe (ORA-Datagroup)	Ja	Nein	Nein	Nein
Datengruppeneinheit (ORA-Datagroupunit)	Ja	Nein	Nein	Nein
Prozessgruppe (ORA-Requestgroup)	Ja	Nein	Nein	Nein
Sicherheitsgruppe (ORA-SecurityGroup)	Ja	Nein	Nein	Nein
Benutzerkonto: Zuweisung an Sicherheitsattribut (ORA-UserHasAttribute)	Ja	Nein	Nein	Nein
Berechtigung (ORA-RESP)	Ja	Nein	Nein	Nein
Zuständigkeit (ORA-Responsibility)	Ja	Nein	Nein	Nein
Zuständigkeit: Ausschlussattribut (ORA-ResponsiExcludesAttribute)	Ja	Nein	Nein	Nein
Zuständigkeit: ausgeschlossenes Menü (ORA-ResponsiExcludesMenu)	Ja	Nein	Nein	Nein
Zuständigkeit: zugewiesenes Sicherheitsattribut (ORA-ResponsiHasAttribute)	Ja	Nein	Nein	Nein

Schematyp	Lesen	Einfügen	Löschen	Aktualisieren
Benutzerkonto: Zuweisung an Berechtigung (ORA-UserInRESPDirect)	Ja	Ja	Nein	Ja
Benutzerkonto: Zuweisung an Berechtigung (ORA-UserInRESPIndirect)	Ja	Nein	Nein	Nein
Person (APSupplierContacts)	Ja	Nein	Nein	Nein
Person (HZParty)	Ja	Nein	Nein	Nein
Person (HRPerson)	Ja	Nein	Nein	Nein
Person (HRPersonManager)	Ja	Nein	Nein	Nein
Standort (HRLocations)	Ja	Nein	Nein	Nein
Sekundäre Zuweisung: Standorte (HRPersonSecondaryLocation)	Ja	Nein	Nein	Nein
Abteilung (HROrganization)	Ja	Nein	Nein	Nein
Sekundäre Zuweisung: Abteilung (HRPersonInOrganization)	Ja	Nein	Nein	Nein

Anhang D

Konfigurationsparameter für die Verwaltung einer Oracle E-Business Suite

Mit der Installation des Moduls sind zusätzlich folgende Konfigurationsparameter im One Identity Manager verfügbar.

Tabelle 55: Konfigurationsparameter

Konfigurationsparameter	Bedeutung
TargetSystem | EBS	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung des Zielsystems Oracle E-Business Suite. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.
TargetSystem | EBS | Accounts	Parameter zur Konfiguration der Angaben zu E-Business Suite Benutzerkonten.
TargetSystem | EBS | 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.
TargetSystem | EBS | Accounts | InitialRandomPassword | SendTo	Angabe, welche Person die 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 die E-Mail an die im Konfigurationsparameter **TargetSystem | EBS | DefaultAddress** hinterlegte Adresse versandt.
TargetSystem | EBS | Accounts | InitialRandomPassword |	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den Anmeldeinformationen zum Benutzerkonto zu versorgen.

Konfigurationsparameter	Bedeutung
SendTo | MailTemplateAccountName	Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto** verwendet.
TargetSystem | EBS | 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 | EBS | 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 | EBS | Accounts | PrivilegedAccount	Der Konfigurationsparameter erlaubt die Konfiguration der Einstellungen für privilegierte Benutzerkonten.
TargetSystem | EBS | Accounts | PrivilegedAccount | AccountName_Postfix	Der Konfigurationsparameter enthält das Postfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem | EBS | Accounts | PrivilegedAccount | AccountName_Prefix	Der Konfigurationsparameter enthält das Präfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem | EBS | DBDeleteOnError	Schlägt das Anlegen eines Benutzerkontos im Zielsystem fehl, so wird bei aktiviertem Konfigurationsparameter das Objekt hinterher aus der Datenbank gelöscht.
TargetSystem | EBS | DefaultAddress	Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem | EBS | MaxFullsyncDuration	Der Konfigurationsparameter enthält die maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.
TargetSystem | EBS | PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest,

Konfigurationsparameter	Bedeutung
	die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem | EBS | PersonAutoDisabledAccounts	Der Konfigurationsparameter legt fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem | EBS | 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 | EBS | 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.

Die folgenden Konfigurationsparameter werden zusätzlich benötigt.

Tabelle 56: Zusätzliche Konfigurationsparameter

Konfigurationsparameter	Bedeutung
Common | Journal | Delete | BulkCount	Anzahl der Einträge, die in einer Operation gelöscht werden sollen.
Common | Journal | Delete | TotalCount	Gesamtmenge der Einträge, die in einem Verarbeitungslauf gelöscht werden sollen.
Common | Journal | LifeTime	Mit diesem Konfigurationsparameter wird die maximale Aufbewahrungszeit (in Tagen) für Einträge des Systemprotokolls in der Datenbank festgelegt. Ältere Einträge werden aus der Datenbank gelöscht.
Common | MailNotification | DefaultSender	Standard E-Mail-Adresse (Absender) zum Versenden von Benachrichtigungen.
DPR | Journal | LifeTime	Der Konfigurationsparameter legt den Aufbewahrungszeitraum (in Tagen) für Synchronisationsprotokolle fest. Ältere Protokolle werden aus der Datenbank gelöscht.
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.

Konfigurationsparameter	Bedeutung
QER | Person | TemporaryDeactivation	Der Konfigurationsparameter legt fest, ob die Benutzerkonten der Person gesperrt werden, wenn die Person zeitweilig oder dauerhaft deaktiviert wird.
QER | Person | UseCentralPassword	Der Konfigurationsparameter legt fest, ob das zentrale Kennwort einer Person in den Benutzerkonten 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.
QER | Structures | Inherite | GroupExclusion	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Wirksamkeit von Berechtigungen. Ist der Parameter aktiviert, können aufgrund von Ausschluss-definitionen die zugewiesenen Berechtigungen reduziert werden. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.

Anhang E

Beispiel für eine Schemaerweiterungsdatei

```
<?xml version="1.0" encoding="utf-8" ?>
<EBSF12>
<ObjectNames>
<Object SchemaName="UserInRESPDirect" ParentSchemaName="ORA-RESPDirect"
DisplayPattern="%vrtDistinguishedName%" IsReadOnly="false" UseDistinct="false">
    <ObjectKey>
        <Key Column="APPS.FND_USER_RESP_GROUPS_DIRECT.USER_ID" IsDNColumn="true"
        X500Abbreviation="UR" />
        <Key Column="APPS.FND_USER_RESP_GROUPS_DIRECT.RESPONSIBILITY_ID" />
        <Key  Column="APPS.FND_USER_RESP_GROUPS_DIRECT.RESPONSIBILITY_APPLICATION_
        ID"  />
        <Key Column="APPS.FND_USER_RESP_GROUPS_DIRECT.SECURITY_GROUP_ID" />
        <Key Column="APPLSYS.FND_APPLICATION.APPLICATION_ID" />
    </ObjectKey>
    <Tables>
        <Table Name="FND_USER_RESP_GROUPS_DIRECT" Schema="APPS" APK="" USN=""
        WhereClause="" >
            <PK Column="SECURITY_GROUP_ID" />
            <PK Column="RESPONSIBILITY_ID" />
            <PK Column="RESPONSIBILITY_APPLICATION_ID" />
            <PK Column="USER_ID" />
        </Table>
        <Table Name="FND_APPLICATION" Schema="APPLSYS" APK="" USN="" WhereClause=""
        JoinParentColumn="APPS.FND_USER_RESP_GROUPS_DIRECT.RESPONSIBILITY_
        APPLICATION_ID" JoinChildColumn="APPLSYS.FND_APPLICATION.APPLICATION_ID" >
```

```
            <PK Column="APPLSYS.FND_APPLICATION.APPLICATION_ID" />
        </Table>
        <Table Name="FND_USER" Schema="APPLSYS" APK="USER_ID" USN="LAST_UPDATE_
        DATE" WhereClause="" JoinParentColumn="APPS.FND_USER_RESP_GROUPS_
        DIRECT.USER_ID" JoinChildColumn="APPLSYS.FND_USER.USER_ID" >
            <PK Column="USER_NAME" />
        </Table>
        <Table Name="FND_SECURITY_GROUPS" Schema="APPLSYS" APK="SECURITY_GROUP_ID"
        USN="LAST_UPDATE_DATE" WhereClause="" JoinParentColumn="APPS.FND_USER_RESP_
        GROUPS_DIRECT.SECURITY_GROUP_ID" JoinChildColumn="APPLSYS.FND_SECURITY_
        GROUPS.SECURITY_GROUP_ID" >
            <PK Column="SECURITY_GROUP_ID" />
        </Table>
        <Table Name="FND_RESPONSIBILITY" Schema="APPLSYS" APK="" USN=""
        WhereClause="" JoinParentColumn="APPS.FND_USER_RESP_GROUPS_
        DIRECT.RESPONSIBILITY_ID, APPS.FND_USER_RESP_GROUPS_DIRECT.RESPONSIBILITY_
        APPLICATION_ID" JoinChildColumn="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_
        ID, APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID" >
            <PK Column="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID" />
            <ParentTableFK Column="APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID"
            ParentColumn="APPLSYS.FND_APPLICATION.APPLICATION_ID" />
        </Table>
    </Tables>
    <Functions>
        <Insert>
            <Function Name="$ebsUserPackageName$.AddResp">
                <Parameter Name="username" PropertyName="APPLSYS.FND_USER.USER_
                NAME" PropertyType="CHAR" Mandatory="TRUE" />
                <Parameter Name="resp_app" PropertyName="APPLSYS.FND_
                APPLICATION.APPLICATION_SHORT_NAME" PropertyType="CHAR"
                Mandatory="TRUE" />
                <Parameter Name="resp_key" PropertyName="APPLSYS.FND_
                RESPONSIBILITY.RESPONSIBILITY_KEY" PropertyType="CHAR"
                Mandatory="TRUE" />
                <Parameter Name="security_group" PropertyName="APPLSYS.FND_
                SECURITY_GROUPS.SECURITY_GROUP_KEY" PropertyType="CHAR"
                Mandatory="TRUE" />
                <Parameter Name="description" PropertyName="APPS.FND_USER_RESP_
                GROUPS_DIRECT.DESCRIPTION" PropertyType="CHAR" Mandatory="TRUE"
                NullValue ="null" />
```

```
            <Parameter Name="start_date" PropertyName="APPS.FND_USER_RESP_
            GROUPS_DIRECT.START_DATE" PropertyType="DATE" Mandatory="TRUE"
            NullValue ="sysdate" />

            <Parameter Name="end_date" PropertyName="APPS.FND_USER_RESP_
            GROUPS_DIRECT.END_DATE" PropertyType="DATE" Mandatory="TRUE"
            NullValue ="null" />

      </Function>

</Insert>

<Update>

      <Function Name="$ebsUserPackageName$.AddResp">

            <Parameter Name="username" PropertyName="APPLSYS.FND_USER.USER_
            NAME" PropertyType="CHAR" Mandatory="TRUE" />

            <Parameter Name="resp_app" PropertyName="APPLSYS.FND_
            APPLICATION.APPLICATION_SHORT_NAME" PropertyType="CHAR"
            Mandatory="TRUE" />

            <Parameter Name="resp_key" PropertyName="APPLSYS.FND_
            RESPONSIBILITY.RESPONSIBILITY_KEY" PropertyType="CHAR"
            Mandatory="TRUE" />

            <Parameter Name="security_group" PropertyName="APPLSYS.FND_
            SECURITY_GROUPS.SECURITY_GROUP_KEY" PropertyType="CHAR"
            Mandatory="TRUE" />

            <Parameter Name="description" PropertyName="APPS.FND_USER_RESP_
            GROUPS_DIRECT.DESCRIPTION" PropertyType="CHAR" Mandatory="TRUE"
            NullValue ="null" />

            <Parameter Name="start_date" PropertyName="APPS.FND_USER_RESP_
            GROUPS_DIRECT.START_DATE" PropertyType="DATE" Mandatory="TRUE"
            NullValue ="sysdate" />

            <Parameter Name="end_date" PropertyName="APPS.FND_USER_RESP_
            GROUPS_DIRECT.END_DATE" PropertyType="DATE" Mandatory="TRUE"
            NullValue ="null" />

      </Function>

</Update>

<Delete>

      <Function Name="$ebsUserPackageName$.DelResp">

            <Parameter Name="username" PropertyName="APPLSYS.FND_USER.USER_
            NAME" PropertyType="CHAR" Mandatory="TRUE" />

            <Parameter Name="resp_app" PropertyName="APPLSYS.FND_
            APPLICATION.APPLICATION_SHORT_NAME" PropertyType="CHAR"
            Mandatory="TRUE" />
```

```
                    <Parameter Name="resp_key" PropertyName="APPLSYS.FND_
                    RESPONSIBILITY.RESPONSIBILITY_KEY" PropertyType="CHAR"
                    Mandatory="TRUE" />
                    <Parameter Name="security_group" PropertyName="APPLSYS.FND_
                    SECURITY_GROUPS.SECURITY_GROUP_KEY" PropertyType="CHAR"
                    Mandatory="TRUE" />
                </Function>
            </Delete>
        </Functions>
</Object>
<\ObjectNames>
</EBSF12>
```

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

G

H

I

J

K

L

M

N

O

P

R

S

V

W

X

Z