One Identity Manager 8.1.5

Administrationshandbuch für die Anbindung einer SharePoint-Umgebung

Legende

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

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

One Identity Manager Administrationshandbuch für die Anbindung einer SharePoint-Umgebung
Aktualisiert - 09. Juli 2021, 13:05 Uhr
Version - 8.1.5

Inhalt

1

Verwalten einer SharePoint Umgebung

Im One Identity Manager können die Komponenten und Zugriffsrechte von SharePoint 2010, SharePoint 2013, SharePoint 2016 und SharePoint 2019 Umgebungen abgebildet werden. Ziel dieser Abbildung ist es, den Mitarbeitern eines Unternehmens Zugriffsrechte auf die Websites einer SharePoint-Umgebung zu gewähren. Für diese Abbildung werden Informationen über folgende Komponenten der SharePoint Umgebung in die One Identity Manager-Datenbank eingelesen.

- die Farm als oberste Ebene der logischen Architektur der SharePoint-Umgebung

  Die SharePoint Farm wird als Basisobjekt für die Synchronisation in der One Identity Manager-Datenbank eingerichtet.
- alle innerhalb der Farm eingerichteten Webanwendungen mit ihren Benutzerrichtlinien und zulässigen Berechtigungen
- alle Websitesammlungen dieser Webanwendungen mit ihren Benutzerkonten und Gruppen
- alle Websites, die innerhalb der Websitesammlungen in einer hierarchischen Struktur angelegt sind (jedoch nicht deren Inhalt)
- alle Berechtigungsstufen und SharePoint Rollen, die die Berechtigungen auf die einzelnen Websites definieren

SharePoint Rollen, Gruppen und Benutzerkonten werden im Kontext der SharePoint-Komponenten abgebildet, für die sie eingerichtet sind. Über diese Objekte werden im One Identity Manager den SharePoint Benutzern die Zugriffsrechte auf die verschiedenen Websites zur Verfügung gestellt. Dafür können Sie die unterschiedlichen Mechanismen des One Identity Managers für die Verbindung der Personen mit ihren SharePoint Benutzerkonten nutzen. Es werden folgende Objekte provisioniert:

- SharePoint Benutzerkonten und ihre Beziehungen zu SharePoint Rollen und Gruppen
- SharePoint Gruppen und ihre Zuordnungen zu Benutzerkonten und Rollen
- SharePoint Rollen und ihre Berechtigungen auf Websites

Für die Anmeldung am SharePoint Server unterstützt der One Identity Manager sowohl die klassische Windows-Authentifizierung als auch die forderungsbasierte Authentifizierung. Jedem SharePoint Benutzerkonto, das sich über die klassische Windows-Authentifizierung

anmelden kann, ist im One Identity Manager ein Active Directory oder LDAP Benutzerkonto bzw. eine Active Directory oder LDAP Gruppe zugeordnet. Voraussetzung dafür ist, dass die zugehörige Active Directory bzw. LDAP-Umgebung ebenfalls in der One Identity Manager-Datenbank abgebildet werden. Informationen über die in der SharePoint-Umgebung genutzten Authentifizierungssyteme können im One Identity Manager gepflegt werden.

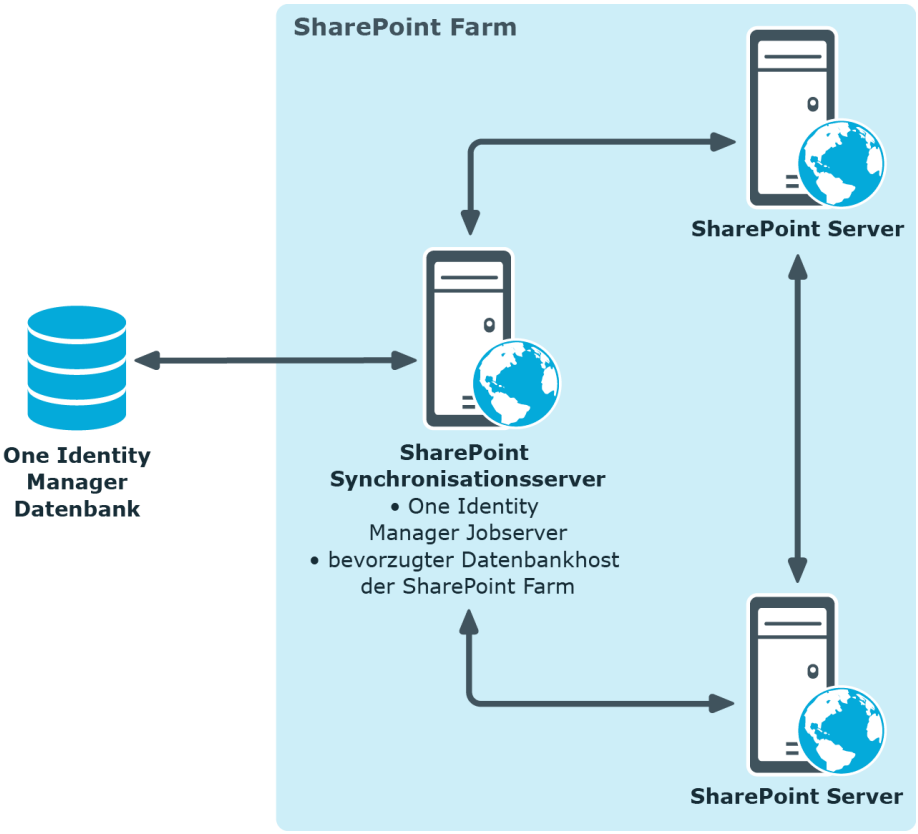
Zu jedem SharePoint Benutzerkonto, das mit einem Active Directory oder LDAP Benutzerkonto verbunden ist, kann zusätzlich eine in der One Identity Manager-Datenbank hinterlegte Person zugeordnet werden. Damit ist es möglich, die Mitgliedschaften von Personen in SharePoint Rollen und Gruppen zu pflegen. Über die Zuordnung von SharePoint Rollen und Gruppen zu den Unternehmensstrukturen können SharePoint Berechtigungen an die Personen vererbt werden. Außerdem ist es möglich, Berechtigungen über den IT Shop zu bestellen. Über Complianceregeln können die einer Person zugewiesenen Berechtigungen überwacht werden.

Das SharePoint Modul basiert auf den SharePoint Foundation 2010, 2013. 2016 beziehungsweise 2019 Class Libraries.

Architekturüberblick

Der SharePoint-Konnektor wird für die Synchronisation und Provisionierung der SharePoint-Umgebung eingesetzt. Der Konnektor kommuniziert direkt mit den SharePoint Servern einer SharePoint Farm.

Abbildung 1: Kommunikationsweg des Konnektors mit der SharePoint-Umgebung



Für die Synchronisation und Provisionierung müssen auf einem beliebigen Server der SharePoint Farm der One Identity Manager Service, der SharePoint Konnektor und der Synchronization Editor installiert sein. Dieser Server wird im Weiteren als Synchronisationsserver bezeichnet. 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.

Detaillierte Informationen zum Thema

- Einrichten des Synchronisationsservers auf Seite 15

One Identity Manager Benutzer für die Verwaltung einer SharePoint-Umgebung

In die Verwaltung einer SharePoint-Umgebung mit dem One Identity Manager 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 | SharePoint** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Systemberechtigungen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Benutzer	Aufgaben
One Identity Manager Administratoren	• Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.
Administratoren für den IT Shop	Die Administratoren müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Systemberechtigungen an IT Shop-Strukturen zu.
Produkteigner für den IT Shop	Die Produkteigner müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Entscheiden über Bestellungen. • Bearbeiten die Leistungspositionen und Service-kategorien, für die sie verantwortlich sind.
Administratoren für Organi-sationen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Organisationen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zu.
Administratoren für Geschäftsrollen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Geschäftsrollen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Systemberechtigungen an Geschäftsrollen zu.

Forderungsbasierte Authentifizierung

Für die Anmeldung am SharePoint Server unterstützt der One Identity Manager sowohl die forderungsbasierte Authentifizierung als auch die klassische Windows-Authentifizierung. Dafür werden in der Datenbank Informationen über die verwendeten SharePoint Provider und Authentifizierungsmodi hinterlegt. Die vorhandenen SharePoint Provider zur forderungsbasierten Authentifizierung müssen durch die Synchronisation in die Datenbank eingelesen werden. Für jede Webanwendung sind die zugelassenen Provider hinterlegt.

An jedem Benutzerkonto ist hinterlegt, mit welchem Authentifizierungsmodus sich der Benutzer mit diesem Benutzerkonto anmeldet. Der standardmäßig zugeordnete Authentifizierungsmodus ist abhängig davon, ob die forderungsbasierte Authentifizierung an der zugehörigen Webanwendung zugelassen ist.

Der Authentifizierungsmodus wird benötigt, um Benutzerkonten im One Identity Manager anzulegen. Der Anmeldename von Benutzerkonten für die forderungsbasierte Authentifizierung enthält ein Präfix, das vom genutzten Authentifizierungsmodus abhängig ist. Diese Präfixe müssen an den Authentifizierungsmodi gepflegt werden.

Verwandte Themen

- Authentifizierungsmodi auf Seite 41

Einrichten der Synchronisation mit einer SharePoint Farm

Um die Objekte einer SharePoint Umgebung initial in die One Identity Manager-Datenbank einzulesen

1. Stellen Sie in der SharePoint-Umgebung ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Die One Identity Manager Bestandteile für die Verwaltung von SharePoint-Umgebungen sind verfügbar, wenn der Konfigurationsparameter "TargetSystem\SharePoint" 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. Synchronisieren Sie die Active Directory oder LDAP Umgebung, auf der die SharePoint Umgebung aufgesetzt ist.

   Ausführliche Informationen zur Synchronisation einer Active Directory Umgebung finden Sie im One Identity Manager Administrationshandbuch für die Anbindung einer Active Directory-Umgebung. Ausführliche Informationen zur Synchronisation einer LDAP Umgebung finden Sie im One Identity Manager Administrationshandbuch für die Anbindung einer LDAP-Umgebung.

   > WICHTIG: Um inkonsistente Daten zu vermeiden, synchronisieren Sie immer zuerst die Active Directory oder LDAP Umgebung, auf der die SharePoint Umgebung aufgesetzt ist. Erst wenn diese Synchronisation erfolgreich abgeschlossen ist, starten Sie die Synchronisation der SharePoint Farm.
   >
   > Wenn das nicht sichergestellt werden kann, definieren Sie unternehmensspezifische Prozesse, um SharePoint Benutzerkonten und Benutzerrichtlinien mit den zugehörigen Authentifizierungsobjekten zu verbinden.
5. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

HINWEIS: Um ein Synchronisationsprojekt zu erstellen oder zu bearbeiten, starten Sie den Synchronization Editor auf dem Synchronisationsserver oder einem Remoteverbindungsserver. Ausführliche Informationen zur Einrichtung einer Remoteverbindung finden Sie im One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation.

Detaillierte Informationen zum Thema

- Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Farm auf Seite 14
- Einrichten des Synchronisationsservers auf Seite 15
- Erstellen eines Synchronisationsprojekts für die initiale Synchronisation einer SharePoint Farm auf Seite 19
- Konfigurationsparameter für die Verwaltung einer SharePoint-Umgebung auf Seite 150

Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Farm

Bei der Synchronisation des One Identity Manager mit einer SharePoint-Umgebung spielen folgende Benutzer ein Rolle.

Tabelle 2: Benutzer für die Synchronisation

Benutzer	Berechtigungen
Benutzer für den Zugriff auf die SharePoint Farm	Für die Anmeldung an der SharePoint Farm während der Synchronisation nutzt der Konnektor das Serverfarmkonto (Farm Account). Stellen sie die Anmeldedaten des Serverfarmkontos bereit. Es kann keine sinnvolle Minimalkonfiguration empfohlen werden, die sich effektiv in ihren Berechtigungen von dem Serverfarmkonto unterscheidet. Die Mitgliedschaft in der Gruppe "Farm Administrators" genügt **nicht**.
Benutzerkonto des One Identity Manager Service	Als Benutzerkonto für den One Identity Manager Service muss das Serverfarmkonto der SharePoint Farm genutzt werden. Das Benutzerkonto für den One Identity Manager Service benötigt zusätzlich die Rechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Rechte vergeben, Verzeichnisse und Dateien anlegen und bearbeiten. Das Benutzerkonto muss der Gruppe **Domänen-Benutzer**

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

Einrichten des Synchronisationsservers

Für die Synchronisation mit einer SharePoint-Umgebung muss ein Synchronisationsserver bereitgestellt werden. Sie können dafür einen beliebigen SharePoint Server der SharePoint Farm nutzen. Auf dem Synchronisationsserver muss die nachfolgend genannte Software installiert sein.

HINWEIS: Ein und derselbe Synchronisationsserver sollte niemals parallel mehrere Synchronisationen ausführen. Verschiedene Synchronisationsserver sollten niemals parallel Synchronisationen für ein und dieselbe SharePoint Farm ausführen.

Wenn Sie die Synchronisation einer SharePoint Farm auf verschiedene Startkonfigurationen aufteilen, stellen Sie sicher, dass diese Startkonfigurationen nacheinander ausgeführt werden. Ausführliche Informationen zum Einrichten von Startkonfigurationen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*. Weitere Informationen finden Sie unter Anpassen einer Synchronisationskonfiguration auf Seite 28.

Um eine SharePoint 2010 Umgebung zu synchronisieren

- Windows Server 2008 R2 (Voraussetzung für SharePoint Server 2010)
- Microsoft SharePoint Server 2010
- Microsoft .NET Framework Version 4.7.2 oder höher

  | HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.
- One Identity Manager Service, SharePoint Konnektor
  - Installieren Sie die One Identity Manager Komponenten mit dem Installationsassistenten.
    1. Wählen Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen**.
    2. Wählen Sie die Maschinenrolle **Server | Jobserver | SharePoint**.

Um eine SharePoint 2013, 2016 oder 2019 Umgebung zu synchronisieren

- Windows Server 2008 R2 oder Windows Server 2012
- Microsoft SharePoint Server 2013, 2016 beziehungsweise 2019
- Microsoft .NET Framework Version 4.7.2 oder höher

  | HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.
- One Identity Manager Service, SharePoint Konnektor
  - Installieren Sie die One Identity Manager Komponenten mit dem Installationsassistenten.
    1. Wählen Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen**.
    2. Wählen Sie die Maschinenrolle **Server | Jobserver | SharePoint**.

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

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 **SharePoint**.
5. Auf der Seite **Serverfunktionen** wählen Sie **SharePoint 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 einem anderen Konto zu starten, deaktivieren Sie die Option **Lokales Systemkonto** und erfassen Sie Benutzerkonto,

Kennwort und Kennwortwiederholung.

Als Benutzerkonto für den One Identity Manager Service muss das Serverfarmkonto der SharePoint Farm genutzt werden.

- **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 Synchronisationsprojekts für die initiale Synchronisation einer SharePoint Farm

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

Ein Synchronisationsprojekt ist die Zusammenstellung aller Informationen, die für die Synchronisation der One Identity Manager-Datenbank mit einem Zielsystem benötigt werden. Dazu gehören die Verbindungsinformationen zum Zielsystem, Schematypen und -eigenschaften, Mappings und Synchronisationsworkflows.

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

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

Tabelle 3: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
SharePoint Version	Der One Identity Manager unterstützt die Synchronisation mit den SharePoint Versionen 2010, 2013, 2016 und 2019.
Benutzername und Kennwort zur Anmeldung an der SharePoint Farm	Um auf die SharePoint Objekte zugreifen zu können, meldet sich der Konnektor mit dem Serverfarmkonto an der SharePoint Farm an. Es werden der Benutzername und das Kennwort des Serverfarmkontos benötigt. Weitere Informationen finden Sie unter Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Farm auf Seite 14.
Domäne	Domäne des Serverfarmkontos.
Synchronisationsserver	Vom Synchronisationsserver werden alle Aktionen des One Identity Manager Service gegen die Zielsystemumgebung ausgeführt. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet. Installierte Komponenten: • SharePoint Server • One Identity Manager Service (gestartet) • Synchronization Editor • SharePoint Konnektor Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt. Weitere Informationen finden Sie unter Einrichten des Synchronisationsservers auf Seite 15.
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 Synchronization Editor nicht direkt auf dem Synchronisationsserver gestartet werden kann, kann eine Remoteverbindung eingerichtet werden. ***Um eine Remoteverbindung zu nutzen***

Angaben	Erläuterungen
	1. Stellen Sie eine Arbeitsstation bereit, auf der der Synchronization Editor installiert ist. 2. Installieren Sie das **RemoteConnectPlugin** auf dem Synchronisationsserver. Damit übernimmt der Synchronisationsserver gleichzeitig die Funktion des Remoteverbindungsservers. 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 • SharePoint Konnektor ist installiert • Zielsystemspezifische Komponenten sind 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*.
Verbindungsdaten zur One Identity Manager-Datenbank	• Datenbankserver • Datenbank • SQL Server Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.

Beim Erstellen eines Synchronisationsprojekts unterstützt Sie ein Assistent. Dieser Assistent führt Sie durch alle Schritte, die zum initialen Einrichten der Synchronisation mit einem Zielsystem erforderlich sind. Wenn Sie alle erforderlichen Angaben für einen Schritt erfasst haben, klicken Sie **Weiter**.

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

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

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

Um ein initiales Synchronisationsprojekt für eine SharePoint Farm einzurichten

1. Starten Sie das Launchpad auf dem Synchronisationsserver 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 SharePoint** 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.
   - Haben Sie das Launchpad auf dem Synchronisationsserver gestartet, nehmen Sie keine Einstellungen vor.
   - Haben Sie das Launchpad auf einer Arbeitsstation gestartet, stellen Sie eine Remoteverbindung her.

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

4. Im Systemverbindungsassistenten erfassen Sie die Verbindungsdaten zur SharePoint Farm. Sie können die Verbindung testen und die Verbindungsdaten speichern.
   - Erfassen Sie folgende Verbindungsdaten.

     Tabelle 4: Verbindungsdaten zur SharePoint Farm

Eigenschaft	Beschreibung
SharePoint Version	Genutzte SharePoint Version.
Domäne	Domäne des Serverfarmkontos.
Benutzername und Kennwort	Benutzername und Kennwort des Serverfarmkontos (Farm Account). Dieses Benutzerkonto wird zur Synchronisation der SharePoint Objekte genutzt.

   - Klicken Sie **Jetzt prüfen**, um die Verbindungsdaten zu prüfen.

     Der Synchronization Editor versucht sich an der SharePoint Farm anzumelden.
   - Um die Verbindungsdaten zu speichern, aktivieren Sie **Verbindung auf dem Computer lokal speichern**. Diese können Sie bei der Einrichtung weiterer Synchronisationsprojekte nutzen.

5. 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.

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

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

   Tabelle 5: Zielsystemzugriff festlegen

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

8. 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.

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

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

Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

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

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

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

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

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

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

HINWEIS: Einige Inhalte erzeugen besonders viele Protokolldaten. Das Synchronisationsprotokoll soll nur die für Fehleranalysen und weitere

Auswertungen notwendigen Daten enthalten.

7. Klicken Sie **OK**.

Um regelmäßige Synchronisationen auszuführen

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

Um die initiale Synchronisation manuell zu starten

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

HINWEIS:

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

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

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie der Websitesammlung die Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand **Linked** (verbunden) die Kontendefinition zu. Es wird der Standardautomatisierungsgrad der Kontendefinition für das Benutzerkonto übernommen.
    a. Wählen Sie im Manager die Kategorie **SharePoint | Benutzerkonten (benutzerauthentifiziert) | Verbunden aber nicht konfiguriert | <Websitesammlung>**.
    b. Wählen Sie im Manager die Kategorie **SharePoint Online | Benutzerkonten (benutzerauthentifiziert) | Verbunden aber nicht konfiguriert | <Websitesammlung>**.
    c. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.

d. Wählen Sie in der Auswahlliste **Kontendefinition** die Kontendefinition.
e. Wählen Sie die Benutzerkonten, die die Kontendefinition erhalten sollen.
f. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Weitere Informationen finden Sie im One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation.

Verwandte Themen

- Einrichten des Synchronisationsservers auf Seite 15
- Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Farm auf Seite 14
- Standardprojektvorlage für SharePoint auf Seite 152
- Einrichten von Kontendefinitionen auf Seite 52
- Automatische Zuordnung von Personen zu SharePoint Benutzerkonten auf Seite 101

Besonderheiten bei der Synchronisation zulässiger Berechtigungen

Zulässige Berechtigungen werden in der One Identity Manager-Datenbank in der Tabelle `SPSWebAppHasPermission` abgebildet; Zuweisungen von zulässigen Berechtigungen an Berechtigungsstufen werden in der Tabelle `SPSRoleHasSPSPermission` abgebildet.

Wenn in der SharePoint-Umgebung eine Berechtigung aus der Liste der zulässigen Berechtigungen für eine Webanwendung entfernt wird, kann diese Berechtigung ab diesem Zeitpunkt keiner Berechtigungsstufe innerhalb der Webanwendung zugewiesen werden. Bereits bestehende Zuweisungen der Berechtigung zu einer Berechtigungsstufe bleiben erhalten, sind jedoch nicht wirksam. Bei der Synchronisation wird diese Berechtigung aus der Tabelle `SPSWebAppHasPermission` gelöscht. Bereits bestehende Zuweisungen der Berechtigung zu einer Berechtigungsstufe werden nicht geändert. Die unwirksamen Berechtigungen werden auf dem Übersichtformular der Berechtigungsstufen angezeigt.

Verwandte Themen

- SharePoint Rollen und Berechtigungsstufen auf Seite 128

Synchronisationsergebnisse anzeigen

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

Um das Protokoll einer Synchronisation anzuzeigen

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

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

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

Um das Protokoll einer Provisionierung anzuzeigen

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

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

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

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

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

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

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

Anpassen einer Synchronisationskonfiguration

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

Um die Datenbank und die SharePoint-Umgebung regelmäßig abzugleichen und Änderungen zu synchronisieren, passen Sie die Synchronisationskonfiguration an.

- Um bei der Synchronisation den One Identity Manager als Mastersystem zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um 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 Farmen eingerichtet werden. Hinterlegen Sie die Verbindungsparameter zur Anmeldung an den Farmen als Variablen.
- Um festzulegen, welche SharePoint Objekte und Datenbankobjekte bei der Synchronisation behandelt werden, bearbeiten Sie den Scope der Zielsystemverbindung und der One Identity Manager-Datenbankverbindung. Um Dateninkonsistenzen zu vermeiden, definieren Sie in beiden Systemen den gleichen Scope. Ist kein Scope definiert, werden alle Objekte synchronisiert.
- 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.

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. Legen Sie als Startverhalten **Mit Fehler abbrechen** oder **Zurückstellen und warten** fest.

Detaillierte Informationen zum Thema

- Synchronisation in die SharePoint-Umgebung konfigurieren auf Seite 29
- Synchronisation verschiedener SharePoint Farmen konfigurieren auf Seite 30
- Schema aktualisieren auf Seite 31
- One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation

Synchronisation in die SharePoint-Umgebung konfigurieren

Das Synchronisationsprojekt für die initiale Synchronisation stellt je einen Workflow zum initialen Einlesen der Zielsystemobjekte (Initial Synchronization) und für die Provisionierung von Objektänderungen aus der One Identity Manager-Datenbank in das Zielsystem (Provisioning) bereit. Um bei der Synchronisation den One Identity Manager als Mastersystem zu nutzen, benötigen Sie zusätzlich einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.

Um eine Synchronisationskonfiguration für die Synchronisation in die SharePoint Farm zu erstellen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.

   TIPP: Um ein bestehendes Synchronisationsprojekt anzupassen, können Sie den Synchronization Editor auf einem beliebigen Server starten. Für die Kommunikation mit den Servern der Farm richten Sie eine Remoteverbindung ein.
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.

Detaillierte Informationen zum Thema

- Synchronisation verschiedener SharePoint Farmen konfigurieren auf Seite 30

Synchronisation verschiedener SharePoint Farmen konfigurieren

Voraussetzungen

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

Um ein Synchronisationsprojekt für die Synchronisation einer weiteren Farm anzupassen

1. Installieren und konfigurieren Sie einen Synchronisationsserver für die weitere Farm. Geben Sie diesen Server im One Identity Manager als Jobserver bekannt.
2. Stellen Sie in der weiteren Farm ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
3. Synchronisieren Sie die Active Directory oder LDAP Umgebung, auf der die weitere Farm aufgesetzt ist.
4. Starten Sie den Synchronization Editor auf dem Synchronisationsserver der weiteren Farm und melden Sie sich an der One Identity Manager-Datenbank an.
5. Öffnen Sie das Synchronisationsprojekt.
6. Erstellen Sie für die weitere Farm ein neues Basisobjekt. Verwenden Sie den Assistenten zur Anlage eines Basisobjektes.
    - Wählen Sie im Assistenten den SharePoint 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.
7. Passen Sie bei Bedarf weitere Komponenten der Synchronisationskonfiguration an.
8. Speichern Sie die Änderungen.
9. Führen Sie eine Konsistenzprüfung durch.

Detaillierte Informationen zum Thema

- Einrichten des Synchronisationsservers auf Seite 15
- Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Farm auf Seite 14
- Synchronisation in die SharePoint-Umgebung konfigurieren auf Seite 29

Schema aktualisieren

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

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

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

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

Um das Schema einer Systemverbindung zu aktualisieren

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

   - ODER -

   Wählen Sie die Kategorie **Konfiguration | One Identity Manager Verbindung**.
3. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Die Schemadaten werden neu geladen.

Um ein Mapping zu bearbeiten

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

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

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

Beschleunigung der Synchronisation durch Revisionsfilterung

Die Synchronisation mit SharePoint unterstützt keine Revisionsfilterung.

Nachbehandlung ausstehender Objekte

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

Ausstehende Objekte

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

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

Führen Sie dafür einen Zielsystemabgleich durch.

Um ausstehende Objekte nachzubearbeiten

1. Wählen Sie im Manager die Kategorie **SharePoint | Zielsystemabgleich: SharePoint**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp **SharePoint** 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 6: 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 .

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

Um kundenspezifische Tabellen in den Zielsystemabgleich aufzunehmen

1. Wählen Sie im Manager die Kategorie **SharePoint | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **SharePoint**.
3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die kundenspezifischen Tabellen zu, für die Sie ausstehende Objekte behandeln möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die kundenspezifischen Tabellen, für die ausstehende Objekte in das Zielsystem publiziert werden dürfen und aktivieren Sie die Option **Publizierbar**.
8. Speichern Sie die Änderungen.

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

Provisionierung von Mitgliedschaften konfigurieren

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

- Mitgliedschaften werden im Zielsystem in Form einer Liste als Eigenschaft eines Objekts gespeichert (Beispiel: Liste von Benutzerkonten in der Eigenschaft `Users` einer `SPGroup`).
- Änderungen von Mitgliedschaften sind in beiden verbundenen Systemen zulässig.
- Ein Provisionierungsworkflow und Provisionierungsprozesse sind eingerichtet.

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

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

Um die Einzelprovisionierung von Mitgliedschaften zu ermöglichen

1. Wählen Sie im Manager die Kategorie **SharePoint | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **SharePoint**.
3. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
4. Wählen Sie die Zuordnungstabellen, für die Sie die Einzelprovisionierung ermöglichen möchten. Mehrfachauswahl ist möglich.
    - Die Option kann nur für Zuordnungstabellen aktiviert werden, deren Basistabelle eine Spalte `XDateSubItem` hat.
    - Zuordnungstabellen, die im Mapping in einer virtuellen Schemaeigenschaft zusammengefasst sind, müssen identisch markiert werden (beispielsweise `SPSGroupHasSPSRLAsgn` und `SPSUserHasSPSRLAsgn`).
5. Klicken Sie **Merge-Modus**.
6. Speichern Sie die Änderungen.

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

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

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

Um die Standardbedingung wiederherzustellen

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

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

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 **SharePoint Konnektor** zu.

   Alle Jobserver müssen auf die gleiche SharePoint Farm zugreifen können, wie der Synchronisationsserver für das jeweilige Basisobjekt.
2. Weisen Sie im Synchronization Editor an das Basisobjekt eine kundendefinierte Serverfunktion zu.

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

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

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

3. Weisen Sie diese Serverfunktion im Manager an alle Jobserver zu, welche die Prozesse zur Provisionierung und Einzelobjektsynchronisation für das Basisobjekt verarbeiten sollen.

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

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

Um den Synchronisationsserver ohne Lastverteilung zu nutzen

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

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

Detaillierte Informationen zum Thema

- Bearbeiten eines Servers auf Seite 44

Unterstützung bei der Analyse von Synchronisationsproblemen

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

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

Um den Synchronisationsanalysebericht zu erstellen

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

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

Deaktivieren der Synchronisation

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

Um regelmäßige Synchronisationen zu verhindern

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

   Synchronisationen können nun nur noch manuell gestartet werden.

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

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

Um das Synchronisationsprojekt zu deaktivieren

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

Detaillierte Informationen zum Thema

- Erstellen eines Synchronisationsprojekts für die initiale Synchronisation einer SharePoint Farm auf Seite 19

3

Basisdaten für die Verwaltung einer SharePoint-Umgebung

Für die Verwaltung von SharePoint-Umgebungen im One Identity Manager sind folgende Basisdaten relevant.

- Konfigurationsparameter

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

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

  Weitere Informationen finden Sie unter Konfigurationsparameter für die Verwaltung einer SharePoint-Umgebung auf Seite 150.

- 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 52.

- Authentifizierungsmodi

  Für die Anmeldung am SharePoint Server unterstützt der One Identity Manager sowohl die forderungsbasierte Authentifizierung als auch die klassische Windows-Authentifizierung. An den Webanwendungen und an den Benutzerkonten ist der verwendete Authentifizierungsmodus hinterlegt. Die nutzbaren Authentifizierungsmodi werden in der One Identity Manager-Datenbank gepflegt.

  Weitere Informationen finden Sie unter Authentifizierungsmodi auf Seite 41.

- Präfixe

  Präfixe sind die relativen URLs einer Webanwendung, unterhalb der Websitesammlungen angelegt werden können.

  Weitere Informationen finden Sie unter Präfixe auf Seite 42.

- Zonen und alternative URLs

  In der One Identity Manager-Datenbank sind alle Zonen hinterlegt, die für eine Webanwendung konfiguriert werden können.

  Weitere Informationen finden Sie unter Zonen und alternative URLs auf Seite 42.

- Webvorlagen

  Webvorlagen werden genutzt, um Websites anzulegen.

  Weitere Informationen finden Sie unter SharePoint Webvorlagen auf Seite 42.

- Berechtigungen

  Über SharePoint Berechtigungen werden Benutzern Berechtigungen auf die Objekte einer SharePoint Website oder einer Webanwendung vergeben. Berechtigungen werden in Berechtigungsstufen und Berechtigungsrichtlinien zusammengefasst.

  Weitere Informationen finden Sie unter SharePoint Berechtigungen auf Seite 43.

- Zielsystemtypen

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

  Weitere Informationen finden Sie unter Nachbehandlung ausstehender Objekte auf Seite 32.

- Server

  Für die Verarbeitung der SharePoint-spezifischen Prozesse im One Identity Manager muss der Synchronisationsserver mit seinen Serverfunktionen bekannt sein.

  Weitere Informationen finden Sie unter Bearbeiten eines Servers auf Seite 44.

- Zielsystemverantwortliche

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

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

  Weitere Informationen finden Sie unter Zielsystemverantwortliche auf Seite 49.

Authentifizierungsmodi

Für die Anmeldung am SharePoint Server unterstützt der One Identity Manager sowohl die forderungsbasierte Authentifizierung als auch die klassische Windows-Authentifizierung. An den Webanwendungen und an den Benutzerkonten ist der verwendete Authentifizierungsmodus hinterlegt. Die nutzbaren Authentifizierungsmodi werden in der One Identity Manager-Datenbank gepflegt. Der One Identity Manager liefert standardmäßig die Authentifizierungsmodi „Windows (Claims)" (= forderungsbasierte Windows-Authentifizierung) und „Windows Classic Mode" (= klassische Windows-Authentifizierung) mit. Wenn in Ihrer SharePoint-Umgebung andere Authentifizierungsmodi zur Anmeldung genutzt werden, legen Sie dafür separate Authentifizierungsmodi im One Identity Manager an. Damit ist eine Zuordnung der Benutzerkonten zu den Authentifizierungsmodi möglich. Erfassen Sie die Informationen zum Benutzerpräfix und Gruppenpräfix. Diese werden benötigt, um neue SharePoint Benutzerkonten im One Identity Manager anzulegen.

Um einen Authentifizierungsmodus anzulegen

1. Wählen Sie die Kategorie **SharePoint | Basisdaten zur Konfiguration | Authentifizierungsmodi**.
2. Klicken Sie in der Ergebnisliste .
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Für einen eigenen Authentifizierungsmodus erfassen Sie folgende Stammdaten.

Tabelle 7: Eigenschaften eines Authentifizierungsmodus

Eigenschaft	Beschreibung
System ID	Beliebige Bezeichnung des Authentifizierungsmodus.
Benutzerpräfix	Präfix zur Bildung eines Anmeldenamens für neue Benutzerkonten. Das zugehörige Authentifizierungsobjekt ist keine Gruppe. Das heißt, am Benutzerkonto ist die Option **Gruppe** deaktiviert.
Gruppenpräfix	Präfix zur Bildung eines Anmeldenamens für neue Benutzerkonten. Das zugehörige Authentifizierungsobjekt ist eine Gruppe. Das heißt, am Benutzerkonto ist die Option **Gruppe** aktiviert.
Spalte für Anmeldename	Spalte aus der Tabelle `Person`, die zur Bildung des Anmeldenamens für neue Benutzerkonten genutzt wird. Diese Information wird benötigt, wenn Personen über die automatische Personenzuordnung mit den Benutzerkonten verbunden werden sollen.

Um einen eigenen Authentifizierungsmodus den Benutzerkonten automatisch zuzuordnen

- Passen Sie im Designer die Bildungsregel für die Spalte `SPSUser.UID_SPSAuthSystem` an.

Weitere Informationen finden Sie im One Identity Manager Konfigurationshandbuch.

Präfixe

Präfixe sind die relativen URLs einer Webanwendung, unterhalb der Websitesammlungen angelegt werden können. Auf dem Überblicksformular werden die Eigenschaften der Präfixe, wie relativer Pfad, absoluter Pfad und Präfixtyp, sowie die zugehörige Webanwendung angezeigt.

Um einen Überblick über ein Präfix zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Basisdaten zur Konfiguration | Präfixe**.
2. Wählen Sie in der Ergebnisliste das Präfix.
3. Wählen Sie die Aufgabe **Überblick über das SharePoint Präfix**.

Zonen und alternative URLs

In der One Identity Manager-Datenbank sind alle Zonen hinterlegt, die für eine Webanwendung konfiguriert werden können. Auf dem Überblicksformular für eine Zone werden die alternativen URLs angezeigt, die für den Zugriff auf die Webanwendungen konfiguriert sind.

Um einen Überblick über eine Zone zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Basisdaten zur Konfiguration | Zonen**.
2. Wählen Sie in der Ergebnisliste die Zone.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Zone**.

Um einen Überblick über die alternativen URLs einer Webanwendung zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | URLs**.
2. Wählen Sie in der Ergebnisliste eine URL.
3. Wählen Sie die Aufgabe **Überblick über die alternative URL**.

SharePoint Webvorlagen

Webvorlagen werden genutzt, um Websites anzulegen. Wenn neue Websites mit dem One Identity Manager angelegt werden sollen, lesen Sie die Webvorlagen durch die

Synchronisation in die One Identity Manager-Datenbank ein. Auf dem Überblicksformular werden die Sprachen angezeigt, in der eine Webvorlage zur Verfügung steht.

Um einen Überblick über eine Webvorlage zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Basisdaten zur Konfiguration | Webvorlagen**.
2. Wählen Sie in der Ergebnisliste die Webvorlage.
3. Wählen Sie die Aufgabe **Überblick über die Webvorlage**.

SharePoint Berechtigungen

Über SharePoint Berechtigungen werden Benutzern Berechtigungen auf die Objekte einer SharePoint Website oder einer Webanwendung vergeben. Berechtigungen werden in Berechtigungsstufen und Berechtigungsrichtlinien zusammengefasst. Auf dem Überblicksformular einer Berechtigung werden alle Berechtigungsrichtlinien der Webanwendungen angezeigt, denen die Berechtigung explizit erteilt oder verweigert wurde.

In einer SharePoint-Umgebung kann die Menge der Berechtigungen, die an Berechtigungsstufen zugewiesen werden kann, eingeschränkt werden. Sie erhalten einen Überblick, für welche Webanwendungen eine Berechtigung zugelassen ist.

Um einen Überblick über eine Berechtigung zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Basisdaten zur Konfiguration | Berechtigungen**.
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Berechtigung**.

Berechtigungen können im One Identity Manager an Berechtigungsstufen zugewiesen werden.

Um eine zulässige Berechtigung an Berechtigungsstufen zuzuweisen

1. Wählen Sie die Kategorie **SharePoint | Basisdaten zur Konfiguration | Berechtigungen**.
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Berechtigungsstufen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungsstufen zu.

   - ODER -

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

Verwandte Themen

- SharePoint Rollen und Berechtigungsstufen auf Seite 128

SharePoint Kontingente

Auf dem Überblicksformular für ein Kontingent werden die SharePoint Farm abgebildet und die Websitesammlungen, denen das Kontingent zugewiesen ist.

Um einen Überblick über ein Kontingent zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Kontingente**.
2. Wählen Sie in der Ergebnisliste das Kontingent.
3. Wählen Sie die Aufgabe **Überblick über das SharePoint Kontingent**.

SharePoint Sprachen

In der One Identity Manager-Datenbank werden alle Sprachen abgebildet, für die in der SharePoint-Umgebung Sprachpakete installiert sind.

Um einen Überblick über eine Sprache zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Sprachen**.
2. Wählen Sie in der Ergebnisliste die Sprache.
3. Wählen Sie die Aufgabe **Überblick über die Sprache**.

Bearbeiten eines Servers

Für die Verarbeitung der SharePoint-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 **SharePoint | Basisdaten zur Konfiguration | Server** einen Eintrag für den Jobserver aus und bearbeiten Sie die Stammdaten des Jobservers.

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

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

Um einen Jobserver und seine Funktionen zu bearbeiten

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

Detaillierte Informationen zum Thema

- Stammdaten eines Jobservers auf Seite 45
- Festlegen der Serverfunktionen auf Seite 47

Verwandte Themen

- Einrichten des Synchronisationsservers auf Seite 15

Stammdaten eines Jobservers

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

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

Tabelle 8: Eigenschaften eines Jobservers

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

Eigenschaft	Bedeutung
Zielsystem	Zielsystem des Computerkontos.
Sprachkultur	Sprache des Servers.
Server ist Cluster	Angabe, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. HINWEIS: Die Eigenschaften **Server ist Cluster** und **Server gehört zu Cluster** schließen einander aus.
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.
IP-Adresse (IPv4)	Internet Protokoll Version 4 (IPv4)-Adresse des Servers.
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. 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

Eigenschaft	Bedeutung
	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 47

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 9: Zulässige Serverfunktionen

Serverfunktion	Anmerkungen
Active Directory Konnektor	Server, auf dem der Active Directory Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem Active Directory aus.
CSV Konnektor	Server, auf dem der CSV Konnektor für die Synchronisation installiert ist.
Domänen-Controller	Active Directory Domänen-Controller. Server, die nicht als Domänen-Controller gekennzeichnet sind, werden als Memberserver betrachtet.
Druckserver	Server, der als Druckserver arbeitet.
Generischer Server	Server für die generische Synchronisation mit einem kundendefinierten Zielsystem.
Homeserver	Server zur Anlage von Homeverzeichnissen für Benutzerkonten.
Aktualisierungsserver	Der Server führt die automatische Softwareaktualisierung aller anderen Server aus. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Der Server kann SQL Aufträge ausführen. Bei der initialen Schemainstallation wird der Server, auf dem die One Identity Manager-Datenbank installiert ist, mit dieser Serverfunktion gekennzeichnet.
SQL Ausführungsserver	Der Server kann SQL Aufträge ausführen. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Für eine Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.
CSV Skriptserver	Der Server kann CSV-Dateien per Prozesskomponente `ScriptComponent` verarbeiten.
Nativer Datenbankkonnektor	Der Server kann sich mit einer ADO.Net Datenbank verbinden.
One Identity Manager-	Server, auf dem der One Identity Manager Konnektor installiert

Serverfunktion	Anmerkungen
Datenbankkonnektor	ist. Dieser Server führt die Synchronisation mit dem Zielsystem One Identity Manager aus.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
Primärer Domänen-Controller	Primärer Domänen-Controller.
Profilserver	Server für die Einrichtung von Profilverzeichnissen für Benutzerkonten.
SAM Synchronisationsserver	Server für die Synchronisation mit einem SMB-basierten Zielsystem aus.
SharePoint Konnektor	Server, auf dem der SharePoint Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem SharePoint aus.
SMTP Host	Server, auf dem durch den One Identity Manager Service E-Mail Benachrichtigungen verschickt werden. Voraussetzung zum Versenden von Mails durch den One Identity Manager Service ist ein konfigurierter SMTP Host.
Standard Berichtserver	Server, auf dem die Berichte generiert werden.
Windows PowerShell Konnektor	Der Server kann Windows PowerShell Version 3.0 oder neuer ausführen.

Verwandte Themen

- Stammdaten eines Jobservers auf Seite 45

Zielsystemverantwortliche

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

Wenn Sie die Bearbeitungsrechte der Zielsystemverantwortlichen auf einzelne SharePoint Farmen 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 SharePoint Farmen 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 SharePoint Farmen zuweisen.

Tabelle 10: Standardanwendungsrolle für Zielsystemverantwortliche

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

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **SharePoint | Farmen**.
3. Wählen Sie in der Ergebnisliste die Farm.
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 | SharePoint** 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, die Farm im One Identity Manager zu bearbeiten.

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer SharePoint-Umgebung auf Seite 9
- Allgemeine Stammdaten einer SharePoint Farm auf Seite 71

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 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*.

HINWEIS: Über Kontendefinitionen können nur SharePoint Benutzerkonten erstellt werden, die nicht als Gruppe gekennzeichnet sind (`IsDomainGroup = 'False'`). Es wird jedoch empfohlen SharePoint Benutzerkonten auf der Basis von Zielsystemgruppen zu erstellen. Nutzen Sie Kontendefintionen für SharePoint nur, wenn Sie nicht dem empfohlenen Vorgehen folgen. Weitere Informationen finden Sie unter SharePoint Benutzerkonten auf Seite 83.

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

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

Erstellen einer Kontendefinition

Um eine Kontendefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **SharePoint | 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 einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 11: 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. TIPP: Sie können hier die Kontendefinition der zugehörigen Active Directory oder LDAP Domäne eintragen. In diesem Fall wird für die Person zunächst ein Active Directory bzw. LDAP Benutzerkonto erzeugt. Ist dieses vorhanden, wird das SharePoint Benutzerkonto angelegt. Dieses Verhalten ist unternehmensspezifisch zu implementieren! Passen Sie den Prozess `TSB_PersonHasAccountDef_AutoCreate_SPSUser` dafür unternehmensspezifisch an.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatisierungsgrad (initial)	Standardautomatisierungsgrad, der bei Neuanlage von Benutzerkonten standardmäßig verwendet werden soll.

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

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

Erstellen der Automatisierungsgrade

Für eine Kontendefinition legen Sie Automatisierungsgrade für die Behandlung der Benutzerkonten fest. Der Automatisierungsgrad eines Benutzerkontos entscheidet über den Umfang der vererbten Eigenschaften der Person an das Benutzerkonto. So kann beispielsweise eine Person mehrere Benutzerkonten in einem Zielsystem besitzen:

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

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

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

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

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

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

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

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

1. Wählen Sie im Manager die Kategorie **SharePoint | 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 **SharePoint | 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 eines Automatisierungsgrades

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 12: 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	Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen gesperrt werden sollen.

Eigenschaft	Beschreibung
Deaktivierung sperren *)	
Gruppen bei verzögertem Löschen beibehalten	Angabe, ob die Benutzerkonten zum Löschen markierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei verzögertem Löschen sperren *)	Angabe, ob die Benutzerkonten zum Löschen markierter Personen gesperrt werden sollen.
Gruppen bei Sicherheitsgefährdung beibehalten	Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei Sicherheitsgefährdung sperren *)	Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen gesperrt werden sollen.
Gruppen bei deaktiviertem Benutzerkonto beibehalten	Angabe, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen.

HINWEIS: SharePoint Benutzerkonten können nicht gesperrt werden!

Wenn eine Person deaktiviert, verzögert gelöscht oder als sicherheitsgefährdend eingestuft wird, bleiben deren SharePoint Benutzerkonten aktiv. Für die Anmeldung an einer SharePoint Websitesammlung ist relevant, ob das als Authentifizierungsobjekt verbundene Benutzerkonto gesperrt bzw. deaktiviert ist. Um zu verhindern, dass sich eine Person, die deaktiviert, gelöscht oder als sicherheitsgefährdend eingestuft ist, an einer SharePoint Websitesammlung anmeldet, verwalten Sie die als Authentifizierungsobjekte verbundenen Benutzerkonten über Kontendefinitionen.

Erstellen einer Abbildungsvorschrift für IT Betriebsdaten

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

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

- SharePoint Authentifizierungsmodus
- SharePoint Online Authentifizierungsmodus
- Gruppen erbbar

- Identität
- Privilegiertes Benutzerkonto

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

1. Wählen Sie im Manager die Kategorie **SharePoint | 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 13: 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

Eigenschaft	Beschreibung
	Mailvorlage zu ändern, passen Sie den Konfigurationsparameter **TargetSystem | SharePoint | Accounts | MailTemplateDefaultValues** an.

4. Speichern Sie die Änderungen.

Erfassen der IT Betriebsdaten

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

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

Beispiel

In der Regel erhält jede Person der Abteilung A ein Standardbenutzerkonto 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 14: 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 **SharePoint | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Bildungsregeln ausführen**.

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

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

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

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinition an Personen

Kontendefinitionen werden an die Personen des Unternehmens zugewiesen.

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

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

aufzunehmen. Diese Systemrollen können über hierarchische Rollen oder direkt an Personen zugewiesen werden oder als Produkte in den IT Shop aufgenommen werden.

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

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

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

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

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

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

Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **SharePoint | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

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

   Um eine Zuweisung zu entfernen

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

Kontendefinition an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

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

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

   Um eine Zuweisung zu entfernen

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

Kontendefinition an alle Personen zuweisen

Um eine Kontendefinition an alle Personen zuzuweisen

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

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

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

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

Kontendefinition direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

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

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

   Um eine Zuweisung zu entfernen

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

Kontendefinition an Systemrollen zuweisen

Installierte Module: Systemrollenmodul

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

Um Kontendefinitionen in eine Systemrolle aufzunehmen

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

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

   Um eine Zuweisung zu entfernen

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

Kontendefinition in den IT Shop aufnehmen

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

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

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

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

Um eine Kontendefinition in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **SharePoint | 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 **SharePoint | 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 **SharePoint | 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 einer Kontendefinition auf Seite 53
- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 63
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 64
- Kontendefinition direkt an Personen zuweisen auf Seite 65
- Kontendefinition an Systemrollen zuweisen auf Seite 65

Zuweisen der Kontendefinition an ein Zielsystem

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

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

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

Um die Kontendefinition an ein Zielsystem zuzuweisen

1. Wählen Sie im Manager in der Kategorie **SharePoint | Websitesammlungen** die Websitesammmlung.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie in der Auswahlliste **Kontendefinition (initial)** die Kontendefinition für die Benutzerkonten.
4. Speichern Sie die Änderungen.

Löschen einer Kontendefinition

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

Um eine Kontendefinition zu löschen

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Personen.
    a. Wählen Sie im Manager die Kategorie **SharePoint | 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 **SharePoint | 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 **SharePoint | 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 **SharePoint | 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 **SharePoint | 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 **SharePoint | 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 **SharePoint | Websitesammlungen** die Websitesammmlung.

   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 **SharePoint | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

   c. Klicken Sie , um die Kontendefinition zu löschen.

4

SharePoint Farmen

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

Um die Stammdaten einer Farm zu bearbeiten

1. Wählen Sie die Kategorie **SharePoint | Farmen**.
2. Wählen Sie in der Ergebnisliste die Farm. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Bearbeiten Sie die Stammdaten der Farm.
4. Speichern Sie die Änderungen.

Allgemeine Stammdaten einer SharePoint Farm

Für eine Farm erfassen Sie folgende allgemeine Stammdaten.

Tabelle 15: Allgemeine Stammdaten einer Farm

Eigenschaft	Beschreibung
Bezeichnung	Name der SharePoint-Instanz. Daraus wird ein definierter Name zur internen Nutzung gebildet.
Domäne	Name der Active Directory oder LDAP Domäne, die als Security Provider für die SharePoint Umgebung dient. Die referenzierten Benutzerkonten und Gruppen werden in dieser Domäne gesucht.
Anzeigename	Anzeigename für die Farm.
Zielsystemverantwortliche	Anwendungsrolle, in der die Zielsystemverantwortlichen der Farm festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte der Farm, der sie zugeordnet

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td></td><td>sind. Jeder Farm können andere Zielsystemverantwortliche zugeordnet werden.

Wählen Sie die One Identity Manager Anwendungsrolle aus, deren Mitglieder verantwortlich für die Administration dieser Farm sind. Über die Schaltfläche  neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.</td></tr>
<tr><td>Synchronisiert durch</td><td>Art der Synchronisation, über welche die Daten zwischen der Farm und dem One Identity Manager ausgetauscht werden. Sobald Objekte für diese Farm im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden.

Beim Erstellen einer Farm mit dem Synchronization Editor wird One Identity Manager verwendet.

Tabelle 16: Zulässige Werte
<table>
<tr><th>Wert</th><th>Synchronisation durch</th><th>Provisionierung durch</th></tr>
<tr><td>One Identity Manager</td><td>SharePoint Konnektor</td><td>SharePoint Konnektor</td></tr>
<tr><td>Keine Synchro-nisation</td><td>keine</td><td>keine</td></tr>
</table>
HINWEIS: Wenn Sie Keine Synchronisation festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.</td></tr>
<tr><td>Build-Version</td><td>Die Build-Version der SharePoint Services dieser Farm wird durch die Synchronisation eingelesen.</td></tr>
</table>

Verwandte Themen

- Zielsystemverantwortliche auf Seite 49

Synchronisationsprojekt bearbeiten

Synchronisationsprojekte, in denen eine Farm bereits als Basisobjekt verwendet wird, können auch über den Manager geöffnet werden. In diesem Modus können beispielsweise die Konfigurationseinstellungen überprüft oder die Synchronisationsprotokolle eingesehen werden. Der Synchronization Editor wird nicht mit seinem vollen Funktionsumfang

gestartet. Verschiedene Funktionen, wie Simulieren oder Ausführen einer Synchronisation, Starten des Zielsystembrowsers und andere, können nicht ausgeführt werden.

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

Um ein bestehendes Synchronisationsprojekt im Synchronization Editor zu öffnen

1. Wählen Sie die Kategorie **SharePoint | Farmen**.
2. Wählen Sie in der Ergebnisliste die Farm. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten...**.

Detaillierte Informationen zum Thema

- One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation

Verwandte Themen

- Anpassen einer Synchronisationskonfiguration auf Seite 28

5

SharePoint Webanwendungen

SharePoint Webanwendungen halten Berechtigungen für SharePoint Benutzer vor, die übergreifend für alle Websites innerhalb der Webanwendung gelten. Über das Überblicksformular erhalten Sie Informationen über die Objekte der SharePoint-Umgebung, in welche die Webanwendung eingebunden ist. Es werden die für die Webanwendung definierten Benutzer- und Berechtigungsrichtlinien angezeigt. An Webanwendungen, für welche die forderungsbasierte Authentifizierung zugelassen ist, werden die zulässigen SharePoint Provider angezeigt.

Im SharePoint kann die Menge der Berechtigungen, die an SharePoint Berechtigungsstufen zugewiesen werden kann, eingeschränkt werden. Auf dem Überblicksformular sehen Sie alle für die Webanwendung zulässigen Berechtigungen.

Um einen Überblick über eine Webanwendung zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Webanwendungen**.
2. Wählen Sie in der Ergebnisliste die Webanwendung.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Webanwendung**.

Verwandte Themen

- SharePoint Rollen und Berechtigungsstufen auf Seite 128

6

SharePoint Websitesammlungen und Websites

SharePoint Websites werden in Websitesammlungen organisiert. Eine Websitesammlung verwaltet Zugriffsrechte und Gestaltungsvorlagen für alle Websites der Websitesammlung. Sie besteht mindestens aus einer Website auf oberster Ebene - der Root-Site. Weitere Websites sind dieser Root-Site untergeordnet. Sie können durch einfache Vorgängerbeziehungen zu Hierarchien verbunden werden. Durch diese hierarchische Struktur können Eigenschaften (beispielsweise Rollendefinitionen) an untergeordnete Websites vererbt werden.

Im One Identity Manager werden Websitesammlungen und Websites mit ihren Zugriffsrechten abgebildet. Ihre Eigenschaften können im One Identity Manager nicht bearbeitet werden. Die innerhalb einer Websitesammlung verwalteten Zugriffsrechte können im One Identity Manager bearbeitet werden. Dafür werden SharePoint Rollen, Gruppen und Benutzerkonten in die One Identity Manager-Datenbank eingelesen.

Verwandte Themen

- SharePoint Rollen und Gruppen auf Seite 107
- SharePoint Benutzerkonten auf Seite 83

SharePoint Websitesammlungen

Eine Websitesammlung fasst die einander untergeordneten Websites zusammen. Hier werden Benutzerkonten und deren Zugriffsberechtigungen auf die Websites verwaltet. Um die automatische Zuordnung von Benutzerkonten und Personen zu nutzen, weisen Sie der Websitesammlung eine Kontendefinition zu.

Auf dem Überblicksformular einer Websitesammlung werden die berechtigten Benutzerkonten und Gruppen dargestellt sowie die Webanwendung und die Root-Site, mit denen die Websitesammlung verbunden ist. Die einer Websitesammlung zugewiesene Kontingentvorlage, die Administratoren und Auditoren der Websitesammlung werden ebenfalls auf dem Überblicksformular abgebildet.

Um die Eigenschaften einer Websitesammlung zu bearbeiten

1. Wählen Sie die Kategorie **SharePoint | Websitesammlungen**.
2. Wählen Sie in der Ergebnisliste die Websitesammlung aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Websitesammlung auf Seite 76
- Festlegen der Kategorien für die Vererbung von SharePoint Gruppen auf Seite 77

Allgemeine Stammdaten einer Websitesammlung

Für Websitesammlungen werden die folgende Stammdaten abgebildet.

Tabelle 17: Allgemeine Stammdaten einer Websitesammlung

Eigenschaft	Beschreibung
Kontendefinition	Initiale Kontendefinition zur Erzeugung von Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für diese Websitesammlung 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.
Server	Name des SharePoint Servers, der die Websitesammlung bereitstellt.
Webanwendung	Eindeutige Kennung der Webanwendung, zu der die Websitesammlung gehört.
Root-Site	Verweis auf die Root-Site dieser Websitesammlung. Es wird auf eine Website verwiesen, bei der die Option **Root-Site** aktiviert ist.
Administrator	Benutzerkonto des Administrators der Websitesammlung.
Zusätzlicher Administrator	Benutzerkonto des zusätzlichen Administrators der Websitesammlung.

Eigenschaft	Beschreibung
Verwendeter Speicherplatz	Information über den Speicherplatz, den die Websitesammlung auf dem Server belegt.
Letzte sicherheitsrelevante Änderung	Zeitpunkt der letzten sicherheitsrelevanten Änderung, die an einem Objekt dieser Websitesammlung vorgenommen wurde.

Auf dem Tabreiter **Adressen** werden die URL und der Port der Websitesammlung angezeigt sowie die URL eines mit der Websitesammlung verbundenen Portals.

Verwandte Themen

- Einrichten von Kontendefinitionen auf Seite 52

Festlegen der Kategorien für die Vererbung von SharePoint Gruppen

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

Um Kategorien zu definieren

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

Detaillierte Informationen zum Thema

- Vererbung von SharePoint Gruppen anhand von Kategorien auf Seite 124
- One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul

SharePoint Websites

Websites können hierarchisch strukturiert werden. Für jede Websitesammlung gibt es immer eine Website, die als „Root-Site" gekennzeichnet ist. Weitere Websites dieser Websitesammlung sind der Root-Site untergeordnet.

Um die Eigenschaften einer Website anzuzeigen

1. Wählen Sie die Kategorie **SharePoint | Websites**.
2. Wählen Sie in der Ergebnisliste die Website. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Website auf Seite 78
- Adressdaten einer Website auf Seite 79
- Designinformationen einer Website auf Seite 80

Allgemeine Stammdaten einer Website

Für Websites werden die folgenden allgemeine Stammdaten abgebildet.

Tabelle 18: Allgemeine Stammdaten einer Website

Eigenschaft	Beschreibung
Anzeigename	Anzeigename der Website.
Root-Site	Angabe, ob die Website die Root-Site der Websitesammlung ist.
Übergeordnete Website	Eindeutige Kennung der übergeordneten Website.
Websitesammlung	Eindeutige Kennung der Websitesammlung, zu der die Website gehört.
Eigene Rollen-definitionen	Angabe, ob Berechtigungsstufen und die damit verbundenen Berechtigungen für die Website definiert werden können (Tabellen `SPSRole` und `SPSRoleHasSPSPermission`). Ist die Option deaktiviert, werden die Rollendefinitionen von der übergeordneten Website geerbt.

Eigenschaft	Beschreibung
Rollen verwenden von	Eindeutige Kennung der Website, deren Rollendefinitionen geerbt werden. Sind der Website eigene Rollen zugewiesen, werden deren Berechtigungen durch die geerbten Berechtigungen überschrieben.
Eigene Rollen-zuweisungen	Angabe, ob Benutzerkonten oder Gruppen direkt auf die Website berechtigt werden können (Tabellen SPSUserHasSPSRLAsgn und SPSGroupHasSPSRLAsgn). Ist die Option deaktiviert, werden die Rollen-zuweisungen von der übergeordneten Website geerbt. Es können keine weiteren Benutzerkonten oder Gruppen auf die Website berechtigt werden.
Zuweisungen verwenden von	Eindeutige Kennung der Website, deren Rollenzuweisungen geerbt werden.
Autor	Verweis auf das Benutzerkonto, mit dem die Website erstellt wurde.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Anonymer Zugriff erlaubt	Angabe, ob ein anonymer Zugriff auf die Website erlaubt ist.

Detaillierte Informationen zum Thema

- SharePoint Rollen und Gruppen auf Seite 107
- SharePoint Rollen und Berechtigungsstufen auf Seite 128

Adressdaten einer Website

Auf dem Tabreiter **Adressen** werden die folgende Adressdaten abgebildet.

Tabelle 19: Adressdaten einer Website

Eigenschaften	Beschreibung
Präfix	Eindeutige Kennung des Präfixes der Websitesammlung, unterhalb der die Website angelegt werden soll. Ein Wert wird nur angezeigt, wenn die Website über den One Identity Manager angelegt wurde.
URL relativ zum Server	URL der Website, relativ zur URL der Webanwendung.
URL	Absolute URL der Website.
URL der Master-seite	URL der Masterseite, die für die Website genutzt wird.
Alternative Master URL	URL zu einer alternativen Masterseite, auf die sich die Website bezieht.
URL des Portals	URL zu einer Portalwebsite, mit der die Website verknüpft ist.

Wenn der in der URL benannte Server per DNS aufgelöst werden kann, können Sie die Website im Standardbrowser öffnen.

Um die Website zu öffnen

1. Wählen Sie die Kategorie **SharePoint | Websites**.
2. Wählen Sie in der Ergebnisliste die Website.
3. Wählen Sie die Aufgabe **URL öffnen**.

Verwandte Themen

- Einrichten von SharePoint Websitesammlungen und Websites auf Seite 81

Designinformationen einer Website

Auf dem Tabreiter **Design** werden die folgende Designinformationen abgebildet.

Tabelle 20: Designinformationen einer Website

Eigenschaft	Beschreibung
Webvorlage	Eindeutige Kennung der Webvorlage, die beim Erstellen der Website genutzt werden soll. Ein Wert wird nur angezeigt, wenn die Website über den One Identity Manager angelegt wurde.
Titel	Bezeichnung, unter der die Website angezeigt wird.
URL zum Logo	URL zum Logo der Website, relativ zur URL der Webanwendung.
Beschreibung zum Logo-Icon	Beschreibung zum Logo der Website.

Verwandte Themen

- Einrichten von SharePoint Websitesammlungen und Websites auf Seite 81

Zusätzliche Aufgaben zur Verwaltung von Websites

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

Auf dem Überblicksformular werden alle für die Website zugelassenen Rollen und Berechtigungsstufen dargestellt. Über die Aufgabe **URL öffnen** können Sie die Website im Standardbrowser öffnen. Voraussetzung dafür ist, dass der in der URL benannte Server per DNS aufgelöst werden kann.

Um einen Überblick über eine Website zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Websites**.
2. Wählen Sie in der Ergebnisliste die Website.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Website**.

Verwandte Themen

- Adressdaten einer Website auf Seite 79

Vererbung von Berechtigungen an untergeordnete Websites

SharePoint Rollen werden auf der Ebene von Websites definiert. Für die Root-Site einer Websitesammlung sind immer Rollen definiert. Untergeordnete Websites können diese Rollendefinitionen erben. Ebenso werden Rollen auf der Root-Site einer Websitesammlung an Gruppen oder Benutzerkonten zugewiesen. Auch diese Zuweisungen können untergeordnete Websites erben. Über die Option **Eigene Rollendefinitionen** ist festgelegt, ob eine Website die Rollen von der übergeordneten Website erbt. Über die Optionen **Eigenen Rollenzuweisungen** ist festgelegt, ob Benutzerkonten und Gruppen auf eine Website explizit berechtigt werden können oder ob die Rollenzuweisungen von der übergeordneten Website geerbt werden.

Detaillierte Informationen zum Thema

- SharePoint Rollen und Gruppen auf Seite 107

Verwandte Themen

- Allgemeine Stammdaten einer Website auf Seite 78

Einrichten von SharePoint Websitesammlungen und Websites

Websitesammlungen und Websites werden in der Standardinstallation des One Identity Manager durch die Synchronisation in die One Identity Manager-Datenbank lediglich eingelesen. Über unternehmensspezifische Anpassungen ist es möglich,

Websitesammlungen und Websites im One Identity Manager neu anzulegen und in die SharePoint-Umgebung zu publizieren. Zu diesem Zweck werden die Spalten UID_SPSPrefix und UID_SPSWebTemplate an der Tabelle SPSWeb sowie vordefinierte Skripte und Prozesse bereitgestellt.

HINWEIS: Folgende Skripte und Prozesse können Sie nutzen, um Websitesammlungen und Websites über den IT Shop bestellbar zu machen. Passen Sie diese Skripte und Prozesse in jedem Fall unternehmensspezifisch an!

Skript/Prozess	Beschreibung
Skript VI_CreateSPSSite	Erstellt eine neue Websitesammlung und die zugehörige Root-Site in der One Identity Manager-Datenbank. Erzeugt ein Benutzerkonto, das als Administrator der Websitesammlung bzw. Autor der Root-Site eingetragen wird.
Skript VI_CreateSPSWeb	Erstellt eine neue Website innerhalb einer Websitesammlung in der One Identity Manager-Datenbank.
Prozess SP0_SPWeb_(De-)Provision	Erstellt eine neue Website innerhalb einer Websitesammlung. Der Prozess wird durch das Ereignis PROVISION ausgelöst, wenn die Website in der One Identity Manager-Datenbank nicht als Root-Site gekennzeichnet ist.
Prozess SP0_SPSite_(De-)Provision	Erstellt eine neue Websitesammlung innerhalb einer Webanwendung und die zugehörige Root-Site. Der Prozess wird durch das Ereignis PROVISION ausgelöst.

Folgende Schritte sind darüber hinaus erforderlich:

- Definieren Sie ein bestellbares Produkt, über das die Websitesammlung/Website im IT Shop bestellt wird.
- Definieren Sie Produkteigenschaften, die auf die Skriptparameter gemappt werden (beispielsweise Webanwendung, Präfix oder Webvorlage). Diese Produkteigenschaften müssen bei der Bestellung der Websitesammlung/Website erfasst werden.
- Erstellen Sie einen Prozess für die Tabelle PersonWantsOrg, der ausgelöst wird, wenn die Bestellung genehmigt wurde (Ereignis OrderGranted). Der Prozess ruft das passende Skript auf und besetzt dessen Parameterwerte mit den definierten Produkteigenschaften. Dadurch wird die Websitesammlung/Website in der One Identity Manager-Datenbank angelegt.

SharePoint Benutzerkonten

SharePoint Benutzerkonten halten die zur Authentifizierung eines Benutzers notwendigen Informationen vor, wie beispielsweise den Authentifizierungsmodus und den Anmeldenamen. Des Weiteren sind an den Benutzerkonten die Berechtigungen der Benutzer innerhalb einer Websitesammlung festgelegt.

Jedes SharePoint Benutzerkonto repräsentiert ein Objekt aus einem Authentifizierungssystem, dem die SharePoint-Installation vertraut. Wenn dieses Authentifizierungssystem als Zielsystem im One Identity Manager verwaltet wird, kann das zur Authentifizierung genutzte Objekt am SharePoint Benutzerkonto als Authentifizierungsobjekt hinterlegt werden. Damit können die Berechtigungen der SharePoint Benutzerkonten auf die im One Identity Manager verwalteten Personen abgebildet werden. Der One Identity Manager schafft damit die Möglichkeit, einen Überblick über alle SharePoint Zugriffsberechtigungen einer Person zu erhalten. SharePoint Berechtigungen können attestiert und Complianceprüfungen durchgeführt werden. Bei entsprechender Konfiguration können Mitarbeiter ihre benötigten SharePoint Berechtigungen über ihre Mitgliedschaften in hierarchischen Rolle erhalten oder über das Web Portal bestellen.

Beispiel

Für eine Websitesammlung soll ein Gastzugang eingerichtet werden, der nur zum Lesen berechtigt. Dafür wird ein SharePoint Benutzerkonto angelegt. Diesem Benutzerkonto wird als Authentifizierungsobjekt die Active Directory Gruppe "Guests" zugeordnet. Clara Harris besitzt ein Active Directory Benutzerkonto, das Mitglied dieser Gruppe ist. Damit kann sie sich an der Websitesammlung anmelden und erhält alle Berechtigungen des SharePoint Benutzerkontos.

Jan Bloggs soll ebenfalls einen Gastzugang für die Websitesammlung erhalten. Er besitzt ein Active Directory Benutzerkonto in der selben Domäne. Im Web Portal bestellt er die Mitgliedschaft in der Active Directory Gruppe "Guests". Sobald die Bestellung genehmigt und zugewiesen ist, kann er sich an der Websitesammlung anmelden.

Standardmäßig können im One Identity Manager folgende Objekte als Authentifizierungsobjekte zugeordnet werden:

- Active Directory Gruppen (ADSGroup)
- Active Directory Benutzerkonten (ADSAccount)
- LDAP Gruppen (LDAPGroup)
- LDAP Benutzerkonten (LDAPAccount)

Bei der Synchronisation versucht der One Identity Manager anhand des Anmeldenamens das passende Authentifizierungsobjekt zuzuordnen.

Abhängig vom referenzierten Authentifizierungsobjekt werden SharePoint Zugriffsberechtigungen im One Identity Manager auf unterschiedliche Weise bereitgestellt.

Fall 1: Das Authentifizierungsobjekt ist eine Gruppe. Das Authentifizierungssystem wird im One Identity Manager verwaltet. (Standardfall)

- Das Benutzerkonto repräsentiert eine Active Directory oder LDAP Gruppe. Diese Gruppe kann im One Identity Manager als Authentifizierungsobjekt zugeordnet werden.
- Dem Benutzerkonto kann keine Person zugeordnet werden. Damit kann das Benutzerkonto nur über Direktzuweisung Mitglied in SharePoint Rollen und Gruppen werden.
- Damit sich eine Person am SharePoint-System anmelden kann, benötigt sie ein Active Directory oder LDAP Benutzerkonto. Dieses Benutzerkonto muss Mitglied in der als Authentifizierungsobjekt genutzten Active Directory oder LDAP Gruppe sein.
- Ein neues SharePoint Benutzerkonto kann manuell erstellt werden.
- Das Benutzerkonto kann nicht über eine Kontendefinition verwaltet werden.

Fall 2: Das Authentifizierungsobjekt ist ein Benutzerkonto. Das Authentifizierungssystem wird im One Identity Manager verwaltet.

- Das Benutzerkonto repräsentiert ein Active Directory oder LDAP Benutzerkonto. Dieses Benutzerkonto kann im One Identity Manager als Authentifizierungsobjekt zugeordnet werden.
- Dem SharePoint Benutzerkonto kann eine Person zugeordnet werden. Damit kann das Benutzerkonto über Vererbung und über Direktzuweisung Mitglied in SharePoint Rollen und Gruppen werden.

  Wenn ein Authentifizierungsobjekt zugeordnet ist, wird die verbundene Person über das Authentifizierungsobjekt ermittelt.

  Wenn kein Authentifizierungsobjekt zugeordnet ist, kann die Person automatisch oder manuell zugeordnet werden. Die automatische Personenzuordnung ist abhängig von den Konfigurationsparametern "TargetSystem\SharePoint\PersonAutoFullsync" und "TargetSystem\SharePoint\PersonAutoDefault".
- Ein neues SharePoint Benutzerkonto kann manuell oder über eine Kontendefinition erstellt werden. Das Active Directory oder LDAP Benutzerkonto, das als

Authentifizierungsobjekt genutzt wird, muss zu einer Domäne gehören dem das referenzierte Authentifizierungssystem vertraut.

- Das Benutzerkonto kann über eine Kontendefinition verwaltet werden.

Fall 3: Das Authentifizierungsobjekt ist ein Benutzerkonto. Das Authentifizierungssystem wird nicht im One Identity Manager verwaltet.

- Dem Benutzerkonto kann kein Authentifizierungsobjekt zugeordnet werden.
- Dem Benutzerkonto kann eine Person manuell oder automatisch zugeordnet werden. Damit kann das Benutzerkonto über Vererbung und über Direktzuweisung Mitglied in SharePoint Rollen und Gruppen werden. Die automatische Personenzuordnung ist abhängig von den Konfigurationsparametern "TargetSystem\SharePoint\PersonAutoFullsync" und "TargetSystem\SharePoint\PersonAutoDefault".
- Ein neues SharePoint Benutzerkonto kann manuell oder über eine Kontendefinition erstellt werden. Wenn eine Kontendefinition verwendet wird, müssen die Bildungsregeln für die Spalten `SPSUser.LoginName` und `SPSUSer.DisplayName` kundenspezifisch angepasst werden.
- Das Benutzerkonto kann über eine Kontendefinition verwaltet werden.

Die Grundlagen zur Verwaltung von Personen und Benutzerkonten sind im One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul beschrieben.

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 21: Identitäten von Benutzerkonten

Identität	Beschreibung	Wert der Spalte IdentityType
Primäre Identität	Standardbenutzerkonto einer Person.	Primary

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

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

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

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

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

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

- Privilegiertes Benutzerkonto

  Privilegierte Benutzerkonten werden eingesetzt, um Personen mit zusätzlichen privilegierten Berechtigungen auszustatten. Dazu gehören beispielsweise

administrative Benutzerkonten oder Dienstkonten. Die Benutzerkonten werden mit der Eigenschaft **Privilegiertes Benutzerkonto** (Spalte `IsPrivilegedAccount`) gekennzeichnet.

Standardbenutzerkonten

In der Regel erhält jede Person ein Standardbenutzerkonto, das die Berechtigungen besitzt, die für die tägliche Arbeit benötigt werden. Die Benutzerkonten haben eine Verbindung zur Person. Die Verbindung zwischen Person und SharePoint Benutzerkonto wird standardmäßig über das Authentifizierungsobjekt hergestellt, das dem Benutzerkonto zugeordnet ist. Davon abweichend können Personen auch direkt mit den Benutzerkonten verbunden sein. Solche Benutzerkonten können über Kontendefinitionen verwaltet werden. Über eine Kontendefinition und deren Automatisierungsgrade kann die Auswirkung der Verbindung und der Umfang der vererbten Eigenschaften der Person an die Benutzerkonten konfiguriert werden.

Um Standardbenutzerkonten über Kontendefinitionen zu erstellen

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

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

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

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

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

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

Administrative Benutzerkonten

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

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

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

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

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

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

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

  Das Benutzerkonto erhält seine Berechtigungen über die Dummy-Person.

Privilegierte Benutzerkonten

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

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

Um privilegierte Benutzerkonten über Kontendefinitionen zu erstellen

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

Kontendefinition zu.

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

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

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

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

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

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

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

Erfassen der Stammdaten für SharePoint Benutzerkonten

Jedes SharePoint Benutzerkonto repräsentiert ein Objekt aus einem Authentifizierungssystem. Dieses Objekt kann eine Gruppe oder ein Benutzer sein. In der Navigationsansicht können die gruppenauthentifizierten und die benutzerauthentifizierten Benutzerkonten separat ausgewählt werden.

Um die Stammdaten eines gruppenauthentifizierten Benutzerkontos zu bearbeiten

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (gruppenauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Um die Stammdaten eines benutzerauthentifizierten Benutzerkontos zu bearbeiten

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Um ein benutzerauthentifiziertes Benutzerkonto für eine Person manuell zuzuweisen oder zu erstellen

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

Detaillierte Informationen zum Thema

- Stammdaten eines gruppenauthentifizierten Benutzerkontos auf Seite 91
- Stammdaten eines benutzerauthentifizierten Benutzerkontos auf Seite 94

Stammdaten eines gruppenauthentifizierten Benutzerkontos

Tabelle 22: Konfigurationsparameter für die Risikobewertung von Benutzerkonten

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

Für ein gruppenauthentifiziertes Benutzerkonto erfassen Sie die folgenden Stammdaten.

Tabelle 23: Stammdaten eines gruppenauthentifizierten Benutzerkontos

Eigenschaft	Beschreibung
Websitesammlung	Websitesammlung, in der das Benutzerkonto genutzt wird.
Gruppenauthentifiziert	Angabe, ob das Authentifizierungsobjekt des Benutzerkontos eine Gruppe ist.
Authentifizierungsobjekt	Authentifizierungsobjekt, welches das Benutzerkonto referenziert. Jedes SharePoint Benutzerkonto repräsentiert ein Objekt aus einem Authentifizierungssystem, dem die SharePoint-Installation vertraut. Wenn dieses Authentifizierungssystem als Zielsystem im One Identity Manager verwaltet wird, kann das zur Authentifizierung genutzte Objekt am SharePoint Benutzerkonto als Authentifizierungsobjekt hinterlegt werden. Das Authentifizierungsobjekt wird bei der Synchronisation automatisch zugeordnet. Beim Einrichten eines neuen Benutzerkontos im Manager, können sie ein Authentifizierungsobjekt zuordnen. Nach dem Speichern kann das Authentifizierungsobjekt nicht mehr geändert werden. Einem gruppenauthentifizierten Benutzerkonto können folgende Authentifizierungsobjekte zugeordnet werden:

Eigenschaft	Beschreibung
	• Active Directory Gruppen mit dem Gruppentyp „Sicherheitsgruppe“ aus der Domäne, die der Farm zugeordnet ist, oder einer Domäne in Vertrauensstellung • LDAP Gruppen aus der Domäne, die der Farm zugeordnet ist
Authentifizierungsmodus	Authentifizierungsmodus, der bei der Anmeldung mit diesem Benutzerkonto am SharePoint Server genutzt wird. Der Anmeldenamen neuer Benutzerkonten ist abhängig vom verwendeten Authentifizierungsmodus. Der Authentifizierungsmodus wird durch eine Bildungsregel gesetzt. Der Wert ist abhängig von der Option **Forderungsauthentifizierung** der zugehörigen Webanwendung. Wenn Sie unternehmensspezifische Authentifizierungsmodi definiert haben, wählen Sie den Authentifizierungsmodus aus der Auswahlliste aus. HINWEIS: Damit ein unternehmensspezifisch angelegter Authentifizierungsmodus an Benutzerkonten zugeordnet werden kann, passen Sie die Bildungsregel für diese Spalte unternehmensspezifisch an (`SPSUser.UID_SPSAuthSystem`).
Anzeigename	Beliebiger Anzeigename des Benutzerkontos. Wird standardmäßig aus dem Anzeigenamen des Authentifizierungsobjektes gebildet. Wenn kein Authentifizierungsobjekt zugeordnet ist, tragen Sie den Anzeigenamen manuell ein.
Anmeldename	Anmeldename des Benutzerkontos. Er wird über eine Bildungsregeln ermittelt. Wenn kein Authentifizierungsobjekt zugeordnet ist, tragen Sie den Anmeldenamen manuell ein. HINWEIS: Damit ein Anmeldename gebildet werden kann, wenn ein unternehmensspezifischer Authentifizierungsmodus zugeordnet ist, passen Sie die Bildungsregel für diese Spalte unternehmensspezifisch an (`SPSUser.LoginName`).
E-Mail-Adresse	E-Mail-Adresse des Benutzerkontos. Sie wird über Bildungsregeln aus der E-Mail-Adresse des Authentifizierungsobjektes gebildet.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten SharePoint Rollen und Gruppen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen an das Benut-

Eigenschaft	Beschreibung
	zerkonto. Gruppen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Hinweise	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.
Administrator	Angabe, ob das Benutzerkonto Administrator einer Websitesammlung ist.
Auditor	Angabe, ob das Benutzerkonto Auditor einer Websitesammlung ist.

Detaillierte Informationen zum Thema

- Authentifizierungsmodi auf Seite 41
- Festlegen der Kategorien für die Vererbung von SharePoint Gruppen auf Seite 77
- Unterstützte Typen von Benutzerkonten auf Seite 85
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

Stammdaten eines benutzerauthentifizierten Benutzerkontos

Tabelle 24: Konfigurationsparameter für die Risikobewertung von Benutzerkonten

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

Für ein benutzerauthentifiziertes Benutzerkonto erfassen Sie die folgenden Stammdaten.

Tabelle 25: Stammdaten eines benutzerauthentifizierten 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 ein Authentifizierungsobjekt zugeordnet ist, wird die verbundene Person per Bildungsregel über das Authentifizierungsobjekt ermittelt. Wenn kein Authentifizierungsobjekt zugeordnet ist, kann die Person automatisch oder manuell zugeordnet werden. 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.
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.
Kontendefinition	Kontendefinition, über die das Benutzerkonto erstellt wurde.

Eigenschaft	Beschreibung
	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. HINWEIS: Sollen Personen ihre SharePoint Benutzerkonten über Kontendefinitionen erhalten, müssen die Personen Benutzerkonten in der Active Directory Domäne oder LDAP Domäne besitzen, die an der SharePoint Farm hinterlegt ist, in der die SharePoint Benutzerkonten erstellt werden sollen.
Websitesammlung	Websitesammlung, in der das Benutzerkonto genutzt wird.
Gruppenauthentifiziert	Angabe, ob das Authentifizierungsobjekt des Benutzerkontos eine Gruppe ist. Die Option ist bei benutzerauthentifizierten Benutzerkonten deaktiviert.
Authentifizierungsobjekt	Authentifizierungsobjekt, welches das Benutzerkonto referenziert. Jedes SharePoint Benutzerkonto repräsentiert ein Objekt aus einem Authentifizierungssystem, dem die SharePoint-Installation vertraut. Wenn dieses Authentifizierungssystem als Zielsystem im One Identity Manager verwaltet wird, kann das zur Authentifizierung genutzte Objekt am SharePoint Benutzerkonto als Authentifizierungsobjekt hinterlegt werden. Das Authentifizierungsobjekt wird bei der Synchronisation automatisch zugeordnet. Beim Einrichten eines neuen Benutzerkontos im Manager, können sie ein Authentifizierungsobjekt zuordnen. Nach dem Speichern kann das Authentifizierungsobjekt nicht mehr geändert werden. Einem benutzerauthentifizierten Benutzerkonto können folgende Authentifizierungsobjekte zugeordnet werden: • Active Directory Benutzerkonten aus der Domäne, die der Farm zugeordnet ist, oder einer Domäne in Vertrauensstellung • LDAP Benutzerkonten aus der Domäne, die der Farm zugeordnet ist Benutzerkonten, die sich auf die Standard-SIDs einer Active Directory Umgebung beziehen, können im One Identity Manager kein Authentifizierungsobjekt referenzieren. HINWEIS: Das SharePoint Benutzerkonto wird auch dann

Eigenschaft	Beschreibung
	erstellt, wenn das Benutzerkonto, das als Authentifizierungsobjekt genutzt wird, deaktiviert oder gesperrt ist.
Authentifizierungsmodus	Authentifizierungsmodus, der bei der Anmeldung mit diesem Benutzerkonto am SharePoint Server genutzt wird. Der Anmeldenamen neuer Benutzerkonten ist abhängig vom verwendeten Authentifizierungsmodus. Der Authentifizierungsmodus wird durch eine Bildungsregel gesetzt. Der Wert ist abhängig von der Option **Forderungsauthentifizierung** der zugehörigen Webanwendung. Wenn Sie unternehmensspezifische Authentifizierungsmodi definiert haben, wählen Sie den Authentifizierungsmodus aus der Auswahlliste aus. HINWEIS: Damit ein unternehmensspezifisch angelegter Authentifizierungsmodus an Benutzerkonten zugeordnet werden kann, passen Sie die Bildungsregel für diese Spalte unternehmensspezifisch an (`SPSUser.UID_SPSAuthSystem`).
Anzeigename	Beliebiger Anzeigename des Benutzerkontos. Wird standardmäßig aus dem Anzeigenamen des Authentifizierungsobjektes gebildet. Wenn kein Authentifizierungsobjekt zugeordnet ist, tragen Sie den Anzeigenamen manuell ein.
Anmeldename	Anmeldename des Benutzerkontos. Er wird über eine Bildungsregeln ermittelt. Wenn kein Authentifizierungsobjekt zugeordnet ist, tragen Sie den Anmeldenamen manuell ein. HINWEIS: Damit ein Anmeldename gebildet werden kann, wenn ein unternehmensspezifischer Authentifizierungsmodus zugeordnet ist, passen Sie die Bildungsregel für diese Spalte unternehmensspezifisch an (`SPSUser.LoginName`).
E-Mail-Adresse	E-Mail-Adresse des Benutzerkontos. Sie wird über Bildungsregeln aus der E-Mail-Adresse des Authentifizierungsobjektes gebildet.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten SharePoint Rollen und Gruppen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen an das Benutzerkonto. Gruppen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der

Eigenschaft	Beschreibung
	Auswahlliste eine oder mehrere Kategorien.
Hinweise	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.
Gruppen erbbar	Angabe, ob das Benutzerkonto SharePoint Rollen und Gruppen über die Person erben darf. Ist die Option aktiviert, werden SharePoint Rollen und Gruppen über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Person eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Gruppe nur, wenn die Option aktiviert ist.
Administrator	Angabe, ob das Benutzerkonto Administrator einer Websitesammlung ist.
Auditor	Angabe, ob das Benutzerkonto Auditor einer Websitesammlung ist.

Detaillierte Informationen zum Thema

- Einrichten von Kontendefinitionen auf Seite 52
- Authentifizierungsmodi auf Seite 41
- Festlegen der Kategorien für die Vererbung von SharePoint Gruppen auf Seite 77
- Automatische Zuordnung von Personen zu SharePoint Benutzerkonten auf Seite 101
- Unterstützte Typen von Benutzerkonten auf Seite 85
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

Zusätzliche Aufgaben zur Verwaltung von SharePoint Benutzerkonten

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

Überblick über das SharePoint Benutzerkonto

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (gruppenauthentifiziert)** oder **SharePoint | Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das SharePoint Benutzerkonto**.

SharePoint Gruppen direkt an ein SharePoint Benutzerkonto zuweisen

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

Es können nur Gruppen aus der Websitesammlung zugewiesen werden, zu der das Benutzerkonto gehört.

Um Gruppen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (gruppenauthentifiziert)** oder **SharePoint | Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- SharePoint Rollen direkt an ein Benutzerkonto zuweisen auf Seite 99
- SharePoint Gruppen an SharePoint Benutzerkonten zuweisen auf Seite 112

SharePoint Rollen direkt an ein Benutzerkonto zuweisen

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

Es können nur SharePoint Rollen aus der Websitesammlung zugewiesen werden, zu der das Benutzerkonto gehört.

HINWEIS: SharePoint Rollen, die auf Berechtigungsstufen verweisen, bei denen die Option **Versteckt** aktiviert ist, können nicht an Benutzerkonten zugewiesen werden.

Um SharePoint Rollen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (gruppenauthentifiziert)** oder **SharePoint | Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.

3. Wählen Sie die Aufgabe**SharePoint Rollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Rollen zu.

   - ODER -

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

Verwandte Themen

- SharePoint Gruppen direkt an ein SharePoint Benutzerkonto zuweisen auf Seite 98
- Erfassen der Stammdaten für SharePoint Berechtigungsstufen auf Seite 129

Zusatzeigenschaften zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (gruppenauthentifiziert)** oder **SharePoint | Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   - ODER -

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

Detaillierte Informationen zum Thema

- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

Unternehmensspezifische Authentifizierungsmodi nutzen

Wenn Benutzerkonten angelegt werden, werden die Werte verschiedener Stammdaten durch Bildungsregeln ermittelt. Bei der Synchronisation versucht der One Identity Manager

ein Authentifizierungsobjekt über die Eigenschaften des Benutzerkontos zu identifizieren und zuzuordnen. Um unternehmensspezifische Authentifizierungsmodi nutzen zu können, müssen die Bildungsregeln verschiedener Spalten gegebenenfalls angepasst werden. Erstellen Sie unternehmensspezifische Bildungsregeln, damit die Authentifizierungsmodi automatisch an Benutzerkonten zugeordnet werden können und Anmeldenamen korrekt gebildet werden.

Um einen unternehmensspezifischen Authentifizierungsmodus zu nutzen

1. Passen Sie im Designer die Bildungsregel für die Spalte `SPSUser.UID_SPSAuthSystem` (Authentifizierungsmodus) an.
2. Prüfen Sie die Bildungsregeln der Spalten `SPSUser.ObjectKeyNamespaceItem` (Authentifizierungsobjekt) und `SPSUser.LoginName` (Anmeldename) und passen Sie diese gegebenenfalls an.

Detaillierte Informationen zum Thema

- Authentifizierungsmodi auf Seite 41
- One Identity Manager Konfigurationshandbuch

Automatische Zuordnung von Personen zu SharePoint Benutzerkonten

Tabelle 26: Konfigurationsparameter für die automatische Personenzuordnung

Konfigurationsparameter	Bedeutung
TargetSystem\SharePoint\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\SharePoint\PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden.

Beim Einfügen eines benutzerauthentifizierten 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.

Voraussetzungen:

- An den Benutzerkonten ist die Option **Gruppenauthentifiziert** deaktiviert.
- Den Benutzerkonten ist kein Authentifizierungsobjekt zugeordnet.

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\SharePoint\PersonAutoFullsync" und wählen Sie den gewünschte Modus aus.
- Wenn Personen außerhalb der Synchronisation zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter „TargetSystem\SharePoint\PersonAutoDefault" und wählen Sie den gewünschten Modus aus.
- Weisen Sie der Websitesammlung 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 der Websitesammlung.

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.

Detaillierte Informationen zum Thema

- Weitere Informationen finden Sie im One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

Verwandte Themen

- Erstellen einer Kontendefinition auf Seite 53
- Zuweisen der Kontendefinition an ein Zielsystem auf Seite 67
- Bearbeiten der Suchkriterien für die automatische Personenzuordnung auf Seite 103

Bearbeiten der Suchkriterien für die automatische Personenzuordnung

Die Kriterien für die Personenzuordnung werden an der Websitesammlung 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 `SPSSite` 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 **SharePoint | Websitesammlungen**.
2. Wählen Sie in der Ergebnisliste die Websitesammlung.
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 27: Standardsuchkriterien für Benutzerkonten

Anwenden auf	Spalte an Person	Spalte am Benutzerkonto
Benutzerkonten (benutzerauthentifiziert)	Zentrales Benutzerkonto (`CentralAccount`)	Anmeldename (`LoginName`)

5. Speichern Sie die Änderungen.

Direkte Zuordnung von Personen an Benutzerkonten anhand einer Vorschlagsliste

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

Tabelle 28: 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.

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

Um die Suchkriterien auf die Benutzerkonten anzuwenden

- Klicken Sie **Neu laden**.

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

Um Personen direkt über die Vorschlagsliste zuzuordnen

1. Klicken Sie **Vorgeschlagene Zuordnungen**.
   a. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die vorgeschlagene Person zugeordnet werden soll. Eine Mehrfachauswahl ist möglich.

b. Klicken Sie **Ausgewählte zuweisen.**

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

Den ausgewählten Benutzerkonten werden die per Suchkriterium ermittelten Personen zugeordnet.

– ODER –

2. Klicken Sie **Ohne Personenzuordnung**.

a. Klicken Sie **Person auswählen** für das Benutzerkonto, dem eine Person zugeordnet werden soll. Wählen Sie eine Person aus der Auswahlliste.

b. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die ausgewählten Personen zugeordnet werden sollen. Eine Mehrfachauswahl ist möglich.

c. Klicken Sie **Ausgewählte zuweisen**.

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

Den ausgewählten Benutzerkonten werden die Personen zugeordnet, die in der Spalte **Person** angezeigt werden.

Um Zuordnungen zu entfernen

1. Klicken Sie **Zugeordnete Benutzerkonten**.

a. Klicken Sie **Auswahl** für alle Benutzerkonten, deren Personenzuordnung entfernt werden soll. Mehrfachauswahl ist möglich.

b. Klicken Sie **Ausgewählte entfernen**.

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

Von den ausgewählten Benutzerkonten werden die zugeordneten Personen entfernt.

Löschen und Wiederherstellen von SharePoint Benutzerkonten

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

Um ein Benutzerkonto zu löschen

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (gruppenauthentifiziert)** oder **SharePoint | Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.

3. Klicken Sie , um das Benutzerkonto zu löschen.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Um ein Benutzerkonto wiederherzustellen

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (gruppenauthentifiziert)** oder **SharePoint | Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste .

Wenn das Authentifizierungsobjekt, das einem SharePoint Benutzerkonto zugeordnet ist, aus der One Identity Manager-Datenbank gelöscht wird, wird der Verweis auf das Authentifizierungsobjekt vom SharePoint Benutzerkonto entfernt. Um dieses Benutzerkonten ebenfalls aus der One Identity Manager-Datenbank zu löschen, definieren Sie unternehmensspezifische Prozesse.

Konfigurieren der Löschverzögerung

Standardmäßig werden Benutzerkonten mit einer Löschverzögerung von 30 Tagen endgültig aus der Datenbank entfernt. Die Benutzerkonten werden zunächst gesperrt. Bis zum Ablauf der Löschverzögerung besteht die Möglichkeit die Benutzerkonten wieder zu aktivieren. Nach Ablauf der Löschverzögerung werden die Benutzerkonten aus der Datenbank gelöscht und ein Wiederherstellen ist nicht mehr möglich. Eine abweichende Löschverzögerung konfigurieren Sie im Designer an der Tabelle SPSUser.

HINWEIS: SharePoint Benutzerkonten können nicht gesperrt werden. Ein Benutzerkonto, das zum Löschen markiert ist, bleibt solange aktiv, bis die Löschverzögerung abgelaufen und das Benutzerkonto endgültig aus der One Identity Manager-Datenbank gelöscht ist.

Sperren Sie das Benutzerkonto, das als Authentifizierungsobjekt mit dem SharePoint Benutzerkonto verbunden ist, um zu verhindern, dass sich ein Benutzer mit einem zum Löschen markierten SharePoint Benutzerkonto an einer Website anmeldet.

8

SharePoint Rollen und Gruppen

SharePoint Berechtigungen werden über SharePoint Rollen und SharePoint Gruppen an Benutzerkonten vererbt. Dabei werden SharePoint Gruppen immer für eine Websitesammlung definiert. SharePoint Rollen werden für Websites definiert. Sie werden an Gruppen zugewiesen und vererben darüber die SharePoint Berechtigungen an die Benutzerkonten, die Mitglied dieser Gruppen sind. SharePoint Rollen können auch direkt an Benutzerkonten zugewiesen werden. Durch die zugewiesenen SharePoint Rollen werden die Berechtigungen der Benutzerkonten auf einzelne Websites einer Websitesammlung eingeschränkt.

Begriffe

- Eine SharePoint Rolle ist die mit einer konkreten Website verknüpfte Berechtigungsstufe.
- Als Rollendefinition wird die Zuweisung von SharePoint Berechtigungen an eine Berechtigungsstufe bezeichnet.
- Die Zuweisung von Benutzerkonten oder Gruppen an eine SharePoint Rolle wird als Rollenzuweisung bezeichnet.

Websites können die Berechtigungen, die die Benutzerkonten auf die Website haben, an untergeordnete Websites vererben. Als übergeordnete Website gilt jede Root-Site einer Websitesammlung sowie jede Website, der eine weitere Website hierarchisch untergeordnet ist. Dabei sind folgende Szenarien möglich:

1. Die untergeordnete Website erbt die Rollendefinitionen und die Rollenzuweisungen.

   Es gelten sowohl die Berechtigungsstufen und Rollendefinitionen als auch die Rollenzuweisungen der übergeordneten (vererbenden) Website. Benutzerkonten und Gruppen können nicht explizit auf die Website berechtigt werden. Es haben nur die Benutzerkonten Zugriff auf diese Website, die auch auf die übergeordnete (vererbende) Website berechtigt sind.

2. Die untergeordnete Website erbt die Rollendefinitionen.

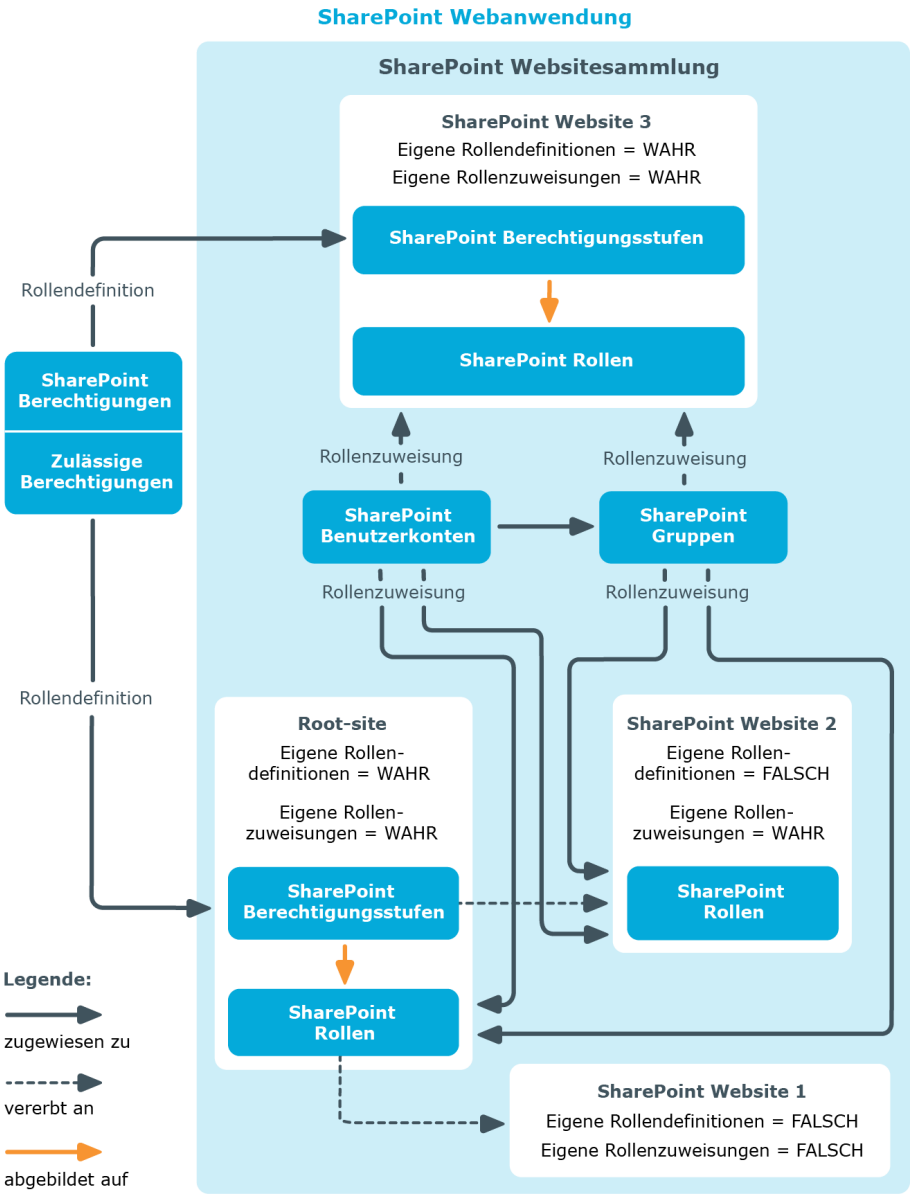
   An der untergeordneten Website können keine eigenen Berechtigungsstufen definiert werden. Die SharePoint Rollen dieser Website verweisen damit auf die Berechtigungsstufen der übergeordneten (vererbenden) Website und deren Rollendefinitionen. Benutzerkonten und Gruppen können an die darauf basierenden SharePoint Rollen der untergeordneten Website zugewiesen werden. Sind an der

untergeordneten Website eigene Berechtigungsstufen definiert, werden deren Berechtigungen durch die geerbten Berechtigungen überschrieben.

3. Die untergeordnete Website erbt weder die Rollendefinitionen noch die Rollenzuweisungen.

   Wie an der Root-Site einer Websitesammlung können hier eigene Berechtigungsstufen mit ihren Rollendefinitionen angelegt werden. Die darauf basierenden SharePoint Rollen werden an Benutzerkonten und Gruppen zugewiesen.

Abbildung 2: Abbildung der Vererbung von SharePoint Berechtigungen an SharePoint Benutzerkonten im One Identity Manager



SharePoint Gruppen

Gruppen werden in SharePoint genutzt, um gleiche Berechtigungen an verschiedene Benutzer zu vergeben. Gruppen werden für eine Websitesammlung angelegt und sind für alle Websites dieser Websitesammlung gültig. Die für eine Website definierten SharePoint Rollen werden direkt an Gruppen zugewiesen. Alle Benutzerkonten, die Mitglied dieser Gruppen sind, erhalten die in den SharePoint Rollen definierten Berechtigungen auf diese Website.

Folgende Informationen über Gruppen können Sie im One Identity Manager bearbeiten:

- Objekteigenschaften wie Anzeigename, Eigentümer oder Sichtbarkeit von Mitgliedschaften
- Zugewiesene SharePoint Rollen und Benutzerkonten
- Nutzung im IT Shop
- Risikobewertung
- Vererbung über hierarchische Rollen und Einschränkung der Vererbung

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie die Kategorie **SharePoint | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Erfassen der Stammdaten für SharePoint Gruppen auf Seite 110

Verwandte Themen

- SharePoint Rollen und Gruppen auf Seite 107

Erfassen der Stammdaten für SharePoint Gruppen

Tabelle 29: Konfigurationsparameter für die Einrichtung von SharePoint Gruppen

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

Für eine Gruppe erfassen Sie die folgenden Stammdaten.

Tabelle 30: Stammdaten einer SharePoint Gruppe

Eigenschaft	Beschreibung
Anzeigename	Anzeigename der Gruppe.
Websitesammlung	Websitesammlung, in der die Gruppe angewendet wird.
Eigentümer	Eigentümer der Gruppe. Es kann entweder ein SharePoint Benutzerkonto oder eine SharePoint Gruppe ausgewählt werden.
Leistungsposition	Angabe einer Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
Alias der Verteilergruppe	Alias der Verteilergruppe, mit der die Gruppe verbunden ist.
E-Mail der Verteilergruppe	E-Mail-Adresse der Verteilergruppe, mit der die Gruppe verbunden ist.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist.
Kategorie	Kategorien für die Vererbung von Gruppen. Gruppen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Beschreibung (HTML)	Zusätzliche Informationen über die Gruppe im HTML-Format. (Wird im SharePoint im Beschreibungsfeld „Über mich“

Eigenschaft	Beschreibung
	angezeigt.)
Nur Gruppenmitglieder dürfen Mitgliedschaften sehen	Angabe, ob nur Mitglieder der Gruppe die Liste der Mitglieder sehen dürfen.
Gruppenmitglieder dürfen Mitgliedschaften bearbeiten	Angabe, ob alle Mitglieder der Gruppe die Mitgliedschaften der Gruppe bearbeiten dürfen.
Benutzer dürfen Mitgliedschaft beantragen	Angabe, ob SharePoint Benutzer die Mitgliedschaft in dieser Gruppe selbst beantragen oder beenden dürfen.
Auf Antrag automatische Mitgliedschaft	Angabe, ob SharePoint Benutzer automatisch Mitglied der Gruppe werden, sobald sie die Mitgliedschaft beantragen. Gleiches gilt, wenn Benutzer die Mitgliedschaft beenden.
E-Mail-Adresse Mitgliedschaftsantrag	E-Mail-Adresse, an die der Antrag auf Mitgliedschaft in der Gruppe beziehungsweise auf Beenden der Mitgliedschaft gesendet wird.
IT Shop	Angabe, ob die Gruppe über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.

Detaillierte Informationen zum Thema

- Festlegen der Kategorien für die Vererbung von SharePoint Gruppen auf Seite 77
- Vererbung von SharePoint Gruppen anhand von Kategorien auf Seite 124
- One Identity Manager Administrationshandbuch für IT Shop
- One Identity Manager Administrationshandbuch für Risikobewertungen

SharePoint Gruppen an SharePoint Benutzerkonten zuweisen

Gruppen können direkt oder indirekt an Personen zugewiesen werden. Bei der indirekten Zuweisung werden Personen und Gruppen in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der Gruppen, die einer Person zugewiesen ist.

Wenn Sie eine Person in hierarchische Rollen aufnehmen und die Person ein benutzerauthentifiziertes Benutzerkonto besitzt, dann wird dieses Benutzerkonto in die Gruppe aufgenommen. Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind:

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und Gruppen erlaubt.
- An den Benutzerkonten ist die Option **Gruppenauthentifiziert** deaktiviert.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.
- Benutzerkonten und Gruppen gehören zur selben Websitesammlung.

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

Detaillierte Informationen zum Thema

- SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 112
- SharePoint Gruppen an Geschäftsrollen zuweisen auf Seite 114
- SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen auf Seite 115
- SharePoint Rollen an SharePoint Gruppen zuweisen auf Seite 116
- SharePoint Gruppen in Systemrollen aufnehmen auf Seite 116
- SharePoint Gruppen in den IT Shop aufnehmen auf Seite 117
- SharePoint Gruppen automatisch in den IT Shop aufnehmen auf Seite 119
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen

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

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

1. Wählen Sie im Manager die Kategorie **SharePoint | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

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

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

   - ODER -

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

   - ODER -

   Wählen Sie im Manager die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **SharePoint Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

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

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

Verwandte Themen

- SharePoint Gruppen an Geschäftsrollen zuweisen auf Seite 114
- SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen auf Seite 115
- SharePoint Rollen an SharePoint Gruppen zuweisen auf Seite 116
- SharePoint Gruppen in Systemrollen aufnehmen auf Seite 116

- SharePoint Gruppen in den IT Shop aufnehmen auf Seite 117
- SharePoint Gruppen automatisch in den IT Shop aufnehmen auf Seite 119
- One Identity Manager Benutzer für die Verwaltung einer SharePoint-Umgebung auf Seite 9

SharePoint Gruppen an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

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

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

1. Wählen Sie im Manager die Kategorie **SharePoint | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

   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 Gruppen an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **SharePoint Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 112
- SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen auf Seite 115
- SharePoint Rollen an SharePoint Gruppen zuweisen auf Seite 116
- SharePoint Gruppen in Systemrollen aufnehmen auf Seite 116
- SharePoint Gruppen in den IT Shop aufnehmen auf Seite 117
- SharePoint Gruppen automatisch in den IT Shop aufnehmen auf Seite 119
- One Identity Manager Benutzer für die Verwaltung einer SharePoint-Umgebung auf Seite 9

SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen

Gruppen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Die indirekte Zuweisung kann nur für benutzerauthentifizierte Benutzerkonten genutzt werden. Die direkte Zuweisung kann für gruppen- und benutzerauthentifizierte Benutzerkonten genutzt werden.

Benutzerkonten und Gruppen müssen zur selben Websitesammlung gehören.

Um eine Gruppe direkt an Benutzerkonten zuzuweisen

1. Wählen Sie die Kategorie **SharePoint | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

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

Verwandte Themen

- SharePoint Gruppen direkt an ein SharePoint Benutzerkonto zuweisen auf Seite 98
- SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 112
- SharePoint Gruppen an Geschäftsrollen zuweisen auf Seite 114
- SharePoint Rollen an SharePoint Gruppen zuweisen auf Seite 116
- SharePoint Gruppen in Systemrollen aufnehmen auf Seite 116

- SharePoint Gruppen in den IT Shop aufnehmen auf Seite 117
- SharePoint Gruppen automatisch in den IT Shop aufnehmen auf Seite 119

SharePoint Rollen an SharePoint Gruppen zuweisen

Damit SharePoint Benutzerkonten Berechtigungen auf die einzelnen Websites erhalten, weisen Sie den Gruppen SharePoint Rollen zu. SharePoint Rollen und Gruppen müssen zur selben Websitesammlung gehören.

HINWEIS: SharePoint Rollen, die auf Berechtigungsstufen verweisen, bei denen die Option **Versteckt** aktiviert ist, können nicht an Gruppen zugewiesen werden.

Um SharePoint Rollen an eine Gruppe zuzuweisen

1. Wählen Sie die Kategorie **SharePoint | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **SharePoint Rollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Rollen zu.

   - ODER -

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

Verwandte Themen

- Erfassen der Stammdaten für SharePoint Berechtigungsstufen auf Seite 129
- SharePoint Gruppen an SharePoint Rollen zuweisen auf Seite 137
- SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 112
- SharePoint Gruppen an Geschäftsrollen zuweisen auf Seite 114
- SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen auf Seite 115
- SharePoint Gruppen in Systemrollen aufnehmen auf Seite 116
- SharePoint Gruppen in den IT Shop aufnehmen auf Seite 117
- SharePoint Gruppen automatisch in den IT Shop aufnehmen auf Seite 119

SharePoint Gruppen in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

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

HINWEIS: Gruppen, 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 Gruppe an Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **SharePoint | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 112
- SharePoint Gruppen an Geschäftsrollen zuweisen auf Seite 114
- SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen auf Seite 115
- SharePoint Rollen an SharePoint Gruppen zuweisen auf Seite 116
- SharePoint Gruppen in den IT Shop aufnehmen auf Seite 117
- SharePoint Gruppen automatisch in den IT Shop aufnehmen auf Seite 119

SharePoint Gruppen in den IT Shop aufnehmen

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

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

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Gruppe im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.

- Soll die Gruppe nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss die Gruppe zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen oder Benutzerkonten ist dann nicht mehr zulässig.

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

Um eine Gruppe in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **SharePoint | Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

Um eine Gruppe aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **SharePoint | Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

Um eine Gruppe aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **SharePoint | Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

5. Klicken Sie **OK**.

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

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

Verwandte Themen

- Erfassen der Stammdaten für SharePoint Gruppen auf Seite 110
- SharePoint Gruppen automatisch in den IT Shop aufnehmen auf Seite 119
- SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 112
- SharePoint Gruppen an Geschäftsrollen zuweisen auf Seite 114
- SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen auf Seite 115
- SharePoint Rollen an SharePoint Gruppen zuweisen auf Seite 116
- SharePoint Gruppen in Systemrollen aufnehmen auf Seite 116

SharePoint Gruppen automatisch in den IT Shop aufnehmen

Tabelle 31: Konfigurationsparameter für die automatische Aufnahme von Gruppen in den IT Shop

Konfigurationsparameter	Beschreibung
QER\ITShop\GroupAutoPublish	Präprozessorrelevanter Konfigurationsparameter zur automatischen Übernahme von Gruppen in den IT Shop. Der Konfigurationsparameter legt fest, ob alle Gruppen der Zielsysteme Active Directory und SharePoint automatisch in den IT Shop übernommen werden. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.

Um Gruppen automatisch in den IT Shop aufzunehmen

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | GroupAutoPublish**.
2. Kompilieren Sie die Datenbank.

Die Gruppen werden ab diesem Zeitpunkt automatisch in den IT Shop aufgenommen.

- Die Synchronisation sorgt dafür, dass die Gruppen in den IT Shop aufgenommen werden. Bei Bedarf können Sie die Synchronisation im Synchronization Editor sofort starten.
- Gruppen, die im One Identity Manager neu erstellt werden, werden in den IT Shop aufgenommen.

Folgende Schritte werden bei der Aufnahme einer Gruppe in den IT Shop automatisch ausgeführt.

1. Es wird eine Leistungsposition für die Gruppe ermittelt.

   Für jede Gruppe wird die Leistungsposition geprüft und bei Bedarf angepasst. Die Bezeichnung der Leistungsposition entspricht der Gruppenbezeichnung. Die Leistungsposition wird einer der Standard-Servicekategorien zugeordnet.

   - Für Gruppen mit Leistungsposition wird die Leistungsposition angepasst.
   - Gruppen ohne Leitungsposition erhalten eine neue Leistungsposition.

2. Es wird eine Anwendungsrolle für Produkteigner ermittelt und der Leistungsposition zugeordnet. Die Produkteigner können Bestellungen von Mitgliedschaften in diesen Gruppen genehmigen. Standardmäßig wird der Eigentümer einer Gruppe als Produkteigner ermittelt.

   HINWEIS: Die Anwendungsrolle für Produkteigner muss der Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner** untergeordnet sein.

   - Ist der Eigentümer der Gruppe bereits Mitglied einer Anwendungsrolle für Produkteigner, dann wird diese Anwendungsrolle der Leistungsposition zugewiesen. Alle Mitglieder dieser Anwendungsrolle werden dadurch Produkteigner der Gruppe.
   - Ist der Eigentümer der Gruppe noch kein Mitglied einer Anwendungsrolle für Produkteigner, dann wird eine neue Anwendungsrolle erzeugt. Die Bezeichnung der Anwendungsrolle entspricht der Bezeichnung des Eigentümers.
     - Handelt es sich beim Eigentümer um ein Benutzerkonto, wird die Person des Benutzerkontos in die Anwendungsrolle aufgenommen.
     - Handelt es sich um eine Gruppe von Eigentümern, werden die Personen aller Benutzerkonten dieser Gruppe in die Anwendungsrolle aufgenommen.
   - Besitzt die Gruppe keine Eigentümer wird die Standard-Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner | Ohne Eigentümer im SharePoint** verwendet.

3. Die Gruppe wird mit der Option **IT Shop** gekennzeichnet und dem IT Shop Regal **SharePoint Gruppen** im Shop **Identity & Access Lifecycle** zugewiesen.

Anschließend können die Kunden des Shops Gruppenmitgliedschaften über das Web Portal bestellen.

HINWEIS: Wenn eine Gruppe endgültig aus der One Identity Manager-Datenbank gelöscht wird, wird auch die zugehörige Leistungsposition gelöscht.

Verwandte Themen

- SharePoint Gruppen in den IT Shop aufnehmen auf Seite 117
- SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 112
- SharePoint Gruppen an Geschäftsrollen zuweisen auf Seite 114
- SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen auf Seite 115
- SharePoint Rollen an SharePoint Gruppen zuweisen auf Seite 116
- SharePoint Gruppen in Systemrollen aufnehmen auf Seite 116
- Standardlösungen für die Bestellung von SharePoint Gruppen auf Seite 127
- One Identity Manager Administrationshandbuch für IT Shop

Zusätzliche Aufgaben für die Verwaltung von SharePoint Gruppen

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

Überblick über die SharePoint Gruppe

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Gruppe.

Um einen Überblick über eine Gruppe zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Gruppe**.

Wirksamkeit von Gruppenmitgliedschaften

Tabelle 32: Konfigurationsparameter für die bedingte Vererbung

Konfigurationsparameter	Wirkung bei Aktivierung
QER | Structures | Inherite | GroupExclusion	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Wirksamkeit von Gruppenmitgliedschaften. Ist der Parameter aktiviert, können aufgrund von Ausschlussdefinitionen die Gruppenmitgliedschaften

Konfigurationsparameter	Wirkung bei Aktivierung
	reduziert werden. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.

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

Die Zuweisung einer ausgeschlossenen Gruppe ist jederzeit direkt, indirekt oder per IT Shop-Bestellung möglich. Anschließend ermittelt der One Identity Manager, ob diese Zuweisung wirksam ist.

HINWEIS:

- Ein wechselseitiger Ausschluss zweier Gruppen kann nicht definiert werden. Das heißt, die Festlegung "Gruppe A schließt Gruppe B aus" UND "Gruppe B schließt Gruppe A aus" ist nicht zulässig.
- Für eine Gruppe muss jede auszuschließende Gruppe einzeln bekannt gegeben werden. Ausschlussdefinitionen werden nicht vererbt.

Die Wirksamkeit der Zuweisungen wird in den Tabellen SPSUserInSPSGroup und BaseTreeHasSPSGroup über die Spalte XIsInEffect abgebildet.

Beispiel für die Wirksamkeit von Gruppenmitgliedschaften

- In einer Websitesammlung sind die Gruppen A, B und C definiert.
- Gruppe A wird über die Abteilung "Marketing", Gruppe B über die Abteilung "Finanzen" und Gruppe C wird über die Geschäftsrolle "Kontrollgruppe" zugewiesen.

Clara Harris hat ein Benutzerkonto in dieser Websitesammlung. Sie gehört primär der Abteilung "Marketing" an. Sekundär sind ihr die Geschäftsrolle "Kontrollgruppe" und die Abteilung "Finanzen" zugewiesen. Ohne Ausschlussdefinition erhält das Benutzerkonto alle Berechtigungen der Gruppen A, B und C.

Durch geeignete Maßnahmen soll verhindert werden, dass eine Person gleichzeitig die Berechtigungen der Gruppe A und der Gruppe B erhält. Das heißt, die Gruppen A und B schließen sich aus. Ein Benutzer, der Mitglied der Gruppe C ist, darf ebenfalls nicht gleichzeitig Mitglied der Gruppe B sein. Das heißt, die Gruppen B und C schließen sich aus.

Tabelle 33: Festlegen der ausgeschlossenen Gruppen (Tabelle `SPSGroupExclusion`)

Wirksame Gruppe	Ausgeschlossene Gruppe
Gruppe A	
Gruppe B	Gruppe A
Gruppe C	Gruppe B

Tabelle 34: Wirksame Zuweisungen

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

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

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

Tabelle 35: Ausgeschlossene Gruppen und wirksame Zuweisungen

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

Voraussetzungen

- Der Konfigurationsparameter **QER | Structures | Inherite | GroupExclusion** ist aktiviert.
- Sich ausschließende Gruppen gehören zur selben Websitesammlung.

Um Gruppen auszuschließen

1. Wählen Sie im Manager die Kategorie **SharePoint | Gruppen**.
2. Wählen Sie in der Ergebnisliste eine Gruppe.
3. Wählen Sie die Aufgabe **Gruppen ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu, die sich mit der gewählten Gruppe ausschließen.

   - ODER -

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

Vererbung von SharePoint Gruppen anhand von Kategorien

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

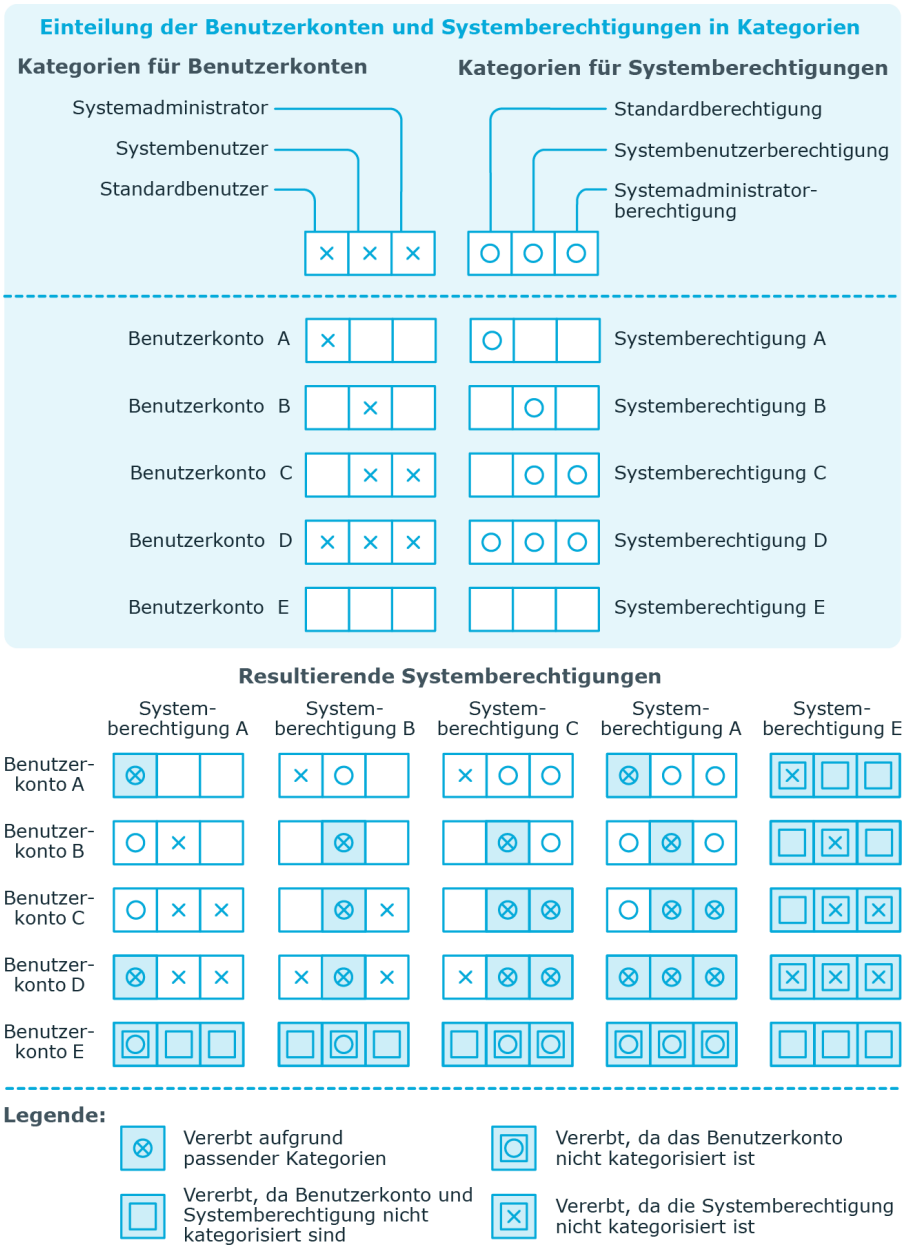
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto vererbt. Ist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

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

Tabelle 36: Beispiele für Kategorien

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

Abbildung 3: Beispiel für die Vererbung über Kategorien



Um die Vererbung über Kategorien zu nutzen

- Definieren Sie an der Websitesammlung die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Gruppen über ihre Stammdaten zu.

Verwandte Themen

- Festlegen der Kategorien für die Vererbung von SharePoint Gruppen auf Seite 77
- Stammdaten eines benutzerauthentifizierten Benutzerkontos auf Seite 94
- Stammdaten eines gruppenauthentifizierten Benutzerkontos auf Seite 91
- Erfassen der Stammdaten für SharePoint Gruppen auf Seite 110

Zusatzeigenschaften an SharePoint Gruppen zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

Um Zusatzeigenschaften für eine Gruppe festzulegen

1. Wählen Sie im Manager die Kategorie **SharePoint | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

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

Löschen von SharePoint Gruppen

Um eine Gruppe zu löschen

1. Wählen Sie die Kategorie **SharePoint | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Klicken Sie , um die Gruppe zu löschen.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Die Gruppe wird endgültig aus der One Identity Manager-Datenbank und der SharePoint-Umgebung gelöscht.

Standardlösungen für die Bestellung von SharePoint Gruppen

Im One Identity Manager werden Standardprodukte und Standard-Entscheidungsworkflows bereitgestellt, um SharePoint Gruppen sowie Mitgliedschaften in diesen Gruppen über den IT Shop zu bestellen. Dadurch werden Berechtigungen in den Zielsystemen über definierte Genehmigungsverfahren vergeben.

Ausführliche Informationen dazu finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

Detaillierte Informationen zum Thema

- Anlegen von SharePoint Gruppen auf Seite 127
- SharePoint Gruppenmitgliedschaften bestellen auf Seite 128

Anlegen von SharePoint Gruppen

Über die Bestellung dieses Standardprodukts können neue SharePoint Gruppen in der SharePoint-Umgebung angelegt werden. Der Besteller gibt Informationen über Namen und Websitesammlung, soweit bekannt, der Bestellung mit. Anhand dieser Informationen bestimmt der Zielsystemverantwortliche die Websitesammlung, in der die Gruppe angelegt werden soll, und genehmigt die Bestellung. Die Gruppe wird im One Identity Manager angelegt und in das Zielsystem publiziert.

Voraussetzung

- Der Anwendungsrolle **Zielsysteme | SharePoint** sind Personen zugewiesen.

Wenn der Konfigurationsparameter **QER | ITShop | GroupAutoPublish** aktiviert ist, wird die Gruppe in den IT Shop aufgenommen und dem Regal **Identity & Access Lifecycle | SharePoint Gruppen** zugewiesen. Die Gruppe wird einer vorhandenen Servicekategorie zugeordnet.

Tabelle 37: Standardprodukt für die Bestellung einer SharePoint Gruppe

Produkt:	Anlegen einer SharePoint Gruppe
Servicekategorie:	SharePoint Gruppen
Regal:	Identity & Access Lifecycle | Gruppen Lifecycle
Entscheidungsrichtlinie/ Entscheidungsworkflow:	Entscheidung der Bestellungen zur Neuanlage von SharePoint Gruppen

Verwandte Themen

- SharePoint Gruppen automatisch in den IT Shop aufnehmen auf Seite 119

SharePoint Gruppenmitgliedschaften bestellen

Produkteigner und Zielsystemverantwortliche können im Web Portal Mitgliedschaften für die Gruppen in diesen Regalen bestellen. Der jeweilige Produkteigner oder Zielsystemverantwortliche muss diese Änderung genehmigen. Die Änderung wird in das Zielsystem publiziert.

Tabelle 38: Standardobjekte für das Bestellen von Gruppenmitgliedschaften

Regale:	Identity & Access Lifecycle | SharePoint Gruppen
Entscheidungsrichtlinien/ Entscheidungsworkflows:	Entscheidung der Bestellungen von Gruppenmitgliedschaften

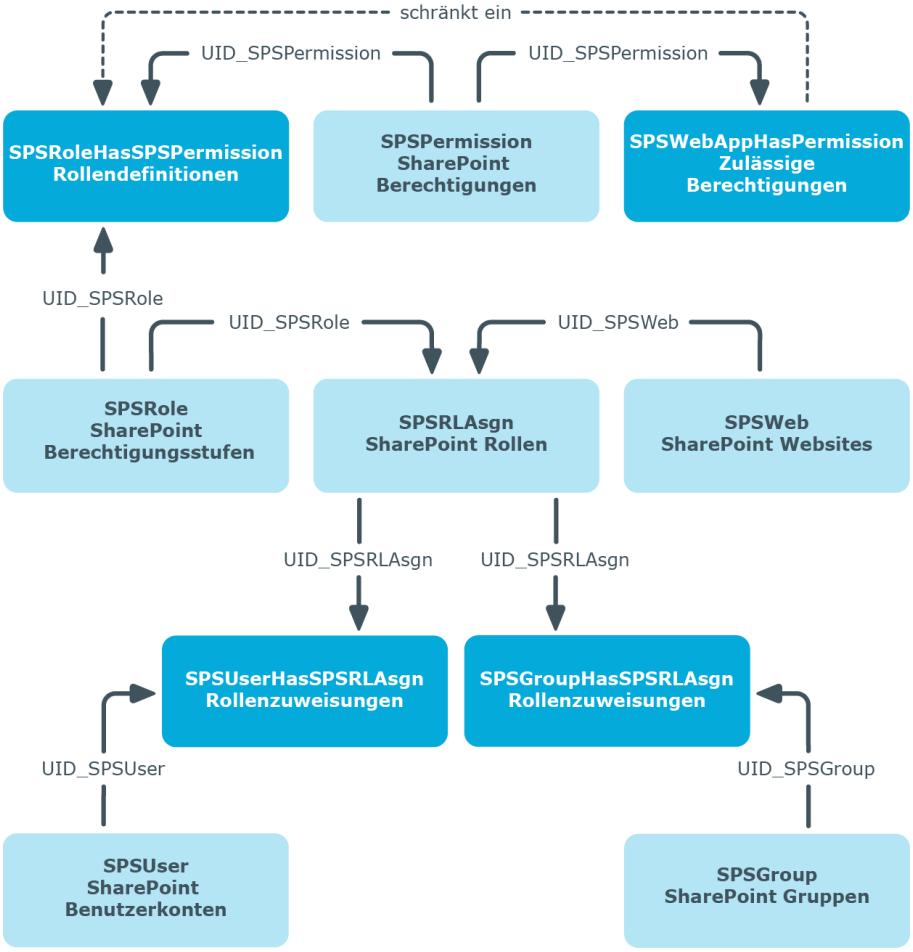
Verwandte Themen

- SharePoint Gruppen automatisch in den IT Shop aufnehmen auf Seite 119
- Anlegen von SharePoint Gruppen auf Seite 127

SharePoint Rollen und Berechtigungsstufen

Um Berechtigungen auf die Objekte einer Website zu vergeben, werden in SharePoint sogenannte Berechtigungsstufen definiert. Diese Berechtigungsstufen fassen verschiedene SharePoint Berechtigungen zusammen. Berechtigungsstufen, die einen eindeutigen Bezug zu einer Website haben, werden in der One Identity Manager-Datenbank als SharePoint Rollen abgebildet. SharePoint Rollen können über Gruppen oder direkt an Benutzerkonten zugewiesen werden. Darüber erhalten die SharePoint Benutzer ihre Berechtigungen auf die Objekte einer Website.

Abbildung 4: Abbildung von SharePoint Rollen und Berechtigungsstufen im One Identity Manager



Erfassen der Stammdaten für SharePoint Berechtigungsstufen

Um die Stammdaten einer Berechtigungsstufe zu bearbeiten

1. Wählen Sie die Kategorie **SharePoint | Berechtigungsstufen**.
2. Wählen Sie in der Ergebnisliste die Berechtigungsstufe. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Für eine Berechtigungsstufe erfassen Sie die folgenden Stammdaten.

Tabelle 39: Eigenschaften einer Berechtigungsstufe

Eigenschaft	Beschreibung
Berechtigungsstufe	Bezeichnung der Berechtigungsstufe.
Website	Eindeutige Kennung der Website, in der die Berechtigungsstufe angelegt ist.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Versteckt	Angabe, ob eine SharePoint Rolle mit dieser Berechtigungsstufe an Benutzerkonten oder Gruppen zugewiesen werden kann.

Zusätzliche Aufgaben für die Verwaltung von SharePoint Berechtigungsstufen

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

Überblick über die SharePoint Berechtigungsstufe

Um einen Überblick über eine Berechtigungsstufe zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Berechtigungsstufen**.
2. Wählen Sie in der Ergebnisliste die Berechtigungsstufe.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Berechtigungsstufe**.

Berechtigungen zuweisen

Im One Identity Manager können Sie SharePoint Berechtigungen an Berechtigungsstufen zuweisen. Dabei können nur die für die Webanwendung zulässigen Berechtigungen zugewiesen werden. Über die SharePoint-internen Vererbungsvorgänge erhalten Benutzerkonten diese Berechtigungen auf eine Website.

Berechtigungen können von anderen Berechtigungen abhängig sein. SharePoint weist diese abhängigen Berechtigungen automatisch zu. Beispielsweise werden mit der Berechtigung "Create Groups" immer auch die Berechtigungen "View Pages", "Browse User Information" und "Open" vergeben werden.

HINWEIS: Abhängige Berechtigungen können im One Identity Manager nicht automatisch an Berechtigungsstufen zugewiesen werden.

Um Berechtigungen an Berechtigungsstufen zuzuweisen

1. Wählen Sie die Kategorie **SharePoint | Berechtigungsstufen**.
2. Wählen Sie in der Ergebnisliste die Berechtigungsstufe.
3. Wählen Sie die Aufgabe **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

- SharePoint Rollen und Gruppen auf Seite 107

Besonderheiten bei der Synchronisation zulässiger Berechtigungen

Wenn in der SharePoint-Umgebung eine Berechtigung aus der Liste der zulässigen Berechtigungen für eine Webanwendung entfernt wird, kann diese Berechtigung ab diesem Zeitpunkt keiner Berechtigungsstufe innerhalb der Webanwendung zugewiesen werden. Bereits bestehende Zuweisungen der Berechtigung zu einer Berechtigungsstufe bleiben erhalten, sind jedoch nicht wirksam. Bei der Synchronisation wird diese Berechtigung aus der Tabelle `SPSWebAppHasPermission` gelöscht. Bereits bestehende Zuweisungen der Berechtigung zu einer Berechtigungsstufe werden nicht geändert. Die unwirksamen Berechtigungen werden auf dem Übersichtformular der Berechtigungsstufen angezeigt.

Erfassen der Stammdaten für SharePoint Rollen

Tabelle 40: Konfigurationsparameter für die Einrichtung von SharePoint Rollen

Konfigurationsparameter	Bedeutung
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.

Um die Stammdaten einer SharePoint Rolle zu bearbeiten

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | <Websitesammlung> | <Website> | Rollen**.
2. Wählen Sie in der Ergebnisliste die SharePoint Rolle. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Für SharePoint Rollen werden die folgenden Stammdaten abgebildet.

Tabelle 41: Eigenschaften einer SharePoint Rolle

Eigenschaft	Beschreibung
Anzeigename	Anzeigename der SharePoint Rolle.
Berechtigungsstufe	Eindeutige Kennung der Berechtigungsstufe, aus der die SharePoint Rolle gebildet ist.
Website	Eindeutige Kennung der Website, an die die SharePoint Rolle ihre Berechtigungen vererbt.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der SharePoint Rolle an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter "QER\CalculateRiskIndex" aktiviert ist.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Leistungsposition	Angabe einer Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
IT Shop	Angabe, ob die SharePoint Rolle über den IT Shop bestellbar ist. Die SharePoint Rolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die SharePoint Rolle kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die SharePoint Rolle ausschließlich über den IT Shop bestellbar ist. Die SharePoint Rolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der SharePoint Rolle an hierarchische Rollen ist nicht zulässig.

HINWEIS: Wenn die SharePoint Rolle auf eine Berechtigungsstufe verweist, bei der die Option **Versteckt** aktiviert ist, können die Optionen **IT Shop** und **Verwendung nur im IT Shop** nicht aktiviert werden. Diese SharePoint Rollen können nicht an Benutzerkonten oder Gruppen zugewiesen werden.

Detaillierte Informationen zum Thema

- Erfassen der Stammdaten für SharePoint Berechtigungsstufen auf Seite 129
- One Identity Manager Administrationshandbuch für IT Shop
- One Identity Manager Administrationshandbuch für Risikobewertungen

SharePoint Rollen an SharePoint Benutzerkonten zuweisen

SharePoint Rollen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Bei der indirekten Zuweisung werden Personen und SharePoint Rollen in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der SharePoint Rollen, die einer Person zugewiesen ist. Wenn Sie eine Person in hierarchische Rollen aufnehmen und die Person ein benutzerauthentifiziertes Benutzerkonto besitzt, dann wird dieses Benutzerkonto in die SharePoint Rolle aufgenommen. Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind:

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und Gruppen erlaubt.
- An den Benutzerkonten ist die Option **Gruppenauthentifiziert** deaktiviert.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.
- Benutzerkonten und SharePoint Rollen gehören zur selben Websitesammlung.

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

HINWEIS: Wenn die SharePoint Rolle auf eine Berechtigungsstufe verweist, bei der die Option **Versteckt** aktiviert ist, können keine Geschäftsrollen und Organisationen zugewiesen werden. Diese SharePoint Rollen können weder direkt noch indirekt an Benutzerkonten oder Gruppen zugewiesen werden.

Detaillierte Informationen zum Thema

- Erfassen der Stammdaten für SharePoint Berechtigungsstufen auf Seite 129
- SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 134
- SharePoint Rollen an Geschäftsrollen zuweisen auf Seite 135
- SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen auf Seite 136
- SharePoint Gruppen an SharePoint Rollen zuweisen auf Seite 137

- SharePoint Rollen in Systemrollen aufnehmen auf Seite 138
- SharePoint Rollen in den IT Shop aufnehmen auf Seite 139
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen

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

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

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | <Websitesammlung> | <Website> | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

   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 SharePoint Rollen an eine Abteilung, eine Kostenstellen oder einen Standorte zuzuweisen (bei rollenbasierter Anmeldung)

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

   - ODER -

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

   - ODER -

   Wählen Sie die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **SharePoint Rollen zuweisen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die SharePoint Rollen zu.

   - ODER -

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

Verwandte Themen

- SharePoint Rollen an Geschäftsrollen zuweisen auf Seite 135
- SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen auf Seite 136
- SharePoint Gruppen an SharePoint Rollen zuweisen auf Seite 137
- SharePoint Rollen in Systemrollen aufnehmen auf Seite 138
- SharePoint Rollen in den IT Shop aufnehmen auf Seite 139
- One Identity Manager Benutzer für die Verwaltung einer SharePoint-Umgebung auf Seite 9

SharePoint Rollen an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

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

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

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | <Websitesammlung> | <Website> | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

   - ODER -

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

Um SharePoint Rollen 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 **SharePoint Rollen zuweisen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die SharePoint Rollen zu.

   - ODER -

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

Verwandte Themen

- SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 134
- SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen auf Seite 136
- SharePoint Gruppen an SharePoint Rollen zuweisen auf Seite 137
- SharePoint Rollen in Systemrollen aufnehmen auf Seite 138
- SharePoint Rollen in den IT Shop aufnehmen auf Seite 139
- One Identity Manager Benutzer für die Verwaltung einer SharePoint-Umgebung auf Seite 9

SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen

SharePoint Rollen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Die indirekte Zuweisung kann nur für benutzerauthentifizierte Benutzerkonten genutzt werden. Die direkte Zuweisung kann für gruppen- und benutzerauthentifizierte Benutzerkonten genutzt werden.

Benutzerkonten und SharePoint Rollen müssen zur selben Websitesammlung gehören.

HINWEIS: Wenn die SharePoint Rolle auf eine Berechtigungsstufe verweist, bei der die Option **Versteckt** aktiviert ist, können keine Benutzerkonten zugewiesen werden.

Um eine SharePoint Rolle direkt an Benutzerkonten zuzuweisen

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | <Websitesammlung> | <Website> | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

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

Verwandte Themen

- Erfassen der Stammdaten für SharePoint Berechtigungsstufen auf Seite 129
- SharePoint Rollen direkt an ein Benutzerkonto zuweisen auf Seite 99
- SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 134
- SharePoint Rollen an Geschäftsrollen zuweisen auf Seite 135
- SharePoint Gruppen an SharePoint Rollen zuweisen auf Seite 137
- SharePoint Rollen in Systemrollen aufnehmen auf Seite 138
- SharePoint Rollen in den IT Shop aufnehmen auf Seite 139

SharePoint Gruppen an SharePoint Rollen zuweisen

Damit SharePoint Benutzerkonten Berechtigungen auf die einzelnen Websites erhalten, weisen Sie den Gruppen SharePoint Rollen zu. SharePoint Rollen und Gruppen müssen zur selben Websitesammlung gehören.

HINWEIS: SharePoint Rollen, die auf Berechtigungsstufen verweisen, bei denen die Option **Versteckt** aktiviert ist, können nicht an Gruppen zugewiesen werden.

Um Gruppen an eine SharePoint Rolle zuzuweisen

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | <Websitesammlung> | <Website> | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

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

Verwandte Themen

- Erfassen der Stammdaten für SharePoint Berechtigungsstufen auf Seite 129
- SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 134
- SharePoint Rollen an Geschäftsrollen zuweisen auf Seite 135
- SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen auf Seite 136
- SharePoint Rollen an SharePoint Gruppen zuweisen auf Seite 116

- SharePoint Rollen in Systemrollen aufnehmen auf Seite 138
- SharePoint Rollen in den IT Shop aufnehmen auf Seite 139

SharePoint Rollen in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

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

HINWEIS: Wenn die SharePoint Rolle auf eine Berechtigungsstufe verweist, bei der die Option **Versteckt** aktiviert ist, können keine Systemrollen zugewiesen werden. Diese SharePoint Rollen können weder direkt nocht indirekt an Benutzerkonten oder Gruppen zugewiesen werden. Weitere Informationen finden Sie unter Erfassen der Stammdaten für SharePoint Berechtigungsstufen auf Seite 129.

HINWEIS: SharePoint Rollen, bei denen die Option **Verwendung nur im IT Shop aktiviert** ist, können nur an Systemrollen zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist. Weitere Informationen finden Sie imOne Identity Manager Administrationshandbuch für Systemrollen.

Um eine SharePoint Rolle an Systemrollen zuzuweisen

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | <Websitesammlung> | <Website> | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 134
- SharePoint Rollen an Geschäftsrollen zuweisen auf Seite 135
- SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen auf Seite 136
- SharePoint Rollen an SharePoint Gruppen zuweisen auf Seite 116
- SharePoint Rollen in den IT Shop aufnehmen auf Seite 139

SharePoint Rollen in den IT Shop aufnehmen

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

- Die SharePoint Rolle muss mit der Option **IT Shop** gekennzeichnet sein.
- Der SharePoint Rolle muss eine Leistungsposition zugeordnet sein.
- Soll die SharePoint Rolle nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss die SharePoint Rolle 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 Administratoren für den IT ShopSharePoint Rollen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt SharePoint Rollen in den IT Shop aufzunehmen.

Um eine SharePoint Rolle in den IT Shop aufzunehmen

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | <Websitesammlung> | <Website> | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine SharePoint Rolle aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | <Websitesammlung> | <Website> | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppe aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine SharePoint Rolle aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | <Websitesammlung> | <Website> | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.

4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

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

Detaillierte Informationen zum Thema

- One Identity Manager Administrationshandbuch für IT Shop

Verwandte Themen

- Erfassen der Stammdaten für SharePoint Rollen auf Seite 131
- SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 134
- SharePoint Rollen an Geschäftsrollen zuweisen auf Seite 135
- SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen auf Seite 136
- SharePoint Gruppen an SharePoint Rollen zuweisen auf Seite 137
- SharePoint Rollen in Systemrollen aufnehmen auf Seite 138

Zusätzliche Aufgaben für die Verwaltung von SharePoint Rollen

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

Überblick über die SharePoint Rolle

Um einen Überblick über eine SharePoint Rolle zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | <Websitesammlung> | <Website> | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Rolle**.

Wirksamkeit von SharePoint Rollen

Das unter Wirksamkeit von Gruppenmitgliedschaften auf Seite 121 beschriebene Verhalten können Sie auch für SharePoint Rollen nutzen.

Die Wirksamkeit der Zuweisungen wird in den Tabellen `SPSUserHasSPSRLAssign` und `BaseTreeHasSPSRLAssign` über die Spalte `XIsInEffect` abgebildet.

Voraussetzungen

- Der Konfigurationsparameter "QER\Structures\Inherite\GroupExclusion" ist aktiviert.
- Sich ausschließende SharePoint Rollen gehören zur selben Websitesammlung.

Um SharePoint Rollen auszuschließen

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | <Websitesammlung> | <Website> | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **SharePoint Rollen ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Rollen zu, die sich mit der gewählten Rolle ausschließen.

   - ODER -

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

Detaillierte Informationen zum Thema

- Wirksamkeit von Gruppenmitgliedschaften auf Seite 121

Löschen von SharePoint Rollen und Berechtigungsstufen

SharePoint Rollen können im Manager nicht gelöscht werden. Sie werden durch den DBQueue Prozessor gelöscht, wenn die zugehörige Berechtigungsstufe gelöscht wird.

Um eine Berechtigungsstufe zu löschen

1. Wählen Sie die Kategorie **SharePoint | Berechtigungsstufen**.
2. Wählen Sie in der Ergebnisliste die Berechtigungsstufe.
3. Klicken Sie , um die Berechtigungsstufe zu löschen.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Wenn eine Löschverzögerung konfiguriert ist, wird die Berechtigungsstufe zum Löschen markiert und erst nach Ablauf der Löschverzögerung endgültig gelöscht. Während dieser Zeit kann die Berechtigungsstufe wiederhergestellt werden. Berechtigungsstufen mit einer Löschverzögerung von 0 Tagen werden sofort gelöscht.

Um eine Berechtigungsstufe wiederherzustellen

1. Wählen Sie die Kategorie **SharePoint | Berechtigungsstufen**.
2. Wählen Sie in der Ergebnisliste die zum Löschen markierte Berechtigungsstufe.
3. Klicken Sie in der Ergebnisliste  .

Verwandte Themen

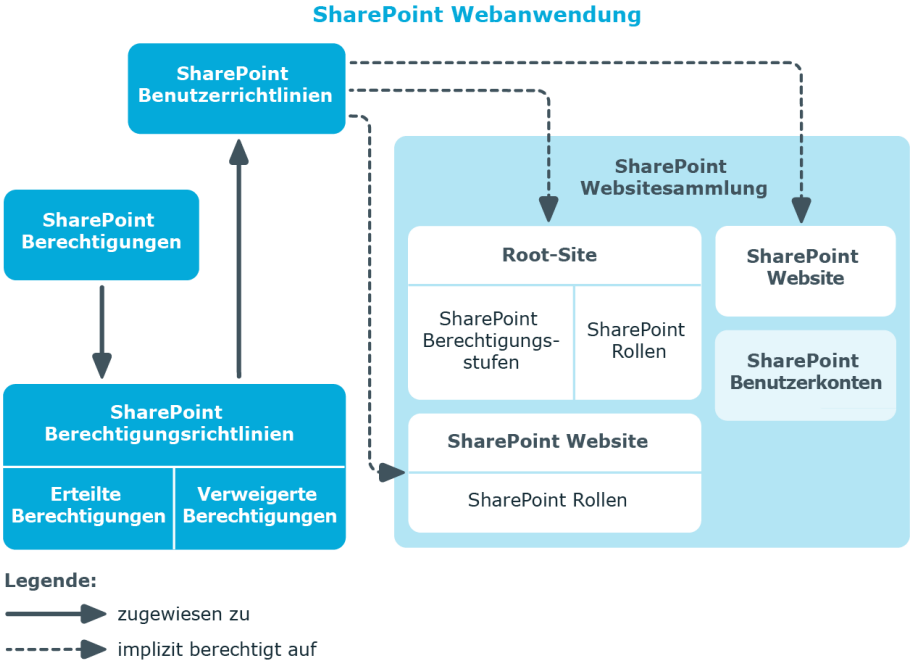
- One Identity Manager Konfigurationshandbuch

Berechtigungen für SharePoint Webanwendungen

In SharePoint können Benutzerrichtlinien definiert werden, um übergreifende Berechtigungen auf alle Websites einer Webanwendung zu gewähren. Diese Benutzerrichtlinien überlagern alle Berechtigungen, die für die Websites speziell definiert wurden. Benutzerrichtlinien basieren auf den Authentifizierungsobjekten, aus denen auch SharePoint Benutzerkonten erzeugt werden. Diese Authentifizierungsobjekte können als Authentifizierungsobjekte an den Benutzerrichtlinien hinterlegt werden.

Benutzerrichtlinien erhalten ihre Berechtigungen über Berechtigungsrichtlinien. In Berechtigungsrichtlinien werden SharePoint Berechtigungen explizit erteilt oder explizit verweigert.

Abbildung 5: Berechtigungen für SharePoint Webanwendungen über Richtlinien



Benutzerrichtlinien und Berechtigungsrichtlinien werden für eine Webanwendung definiert. Benutzerrichtlinien werden dadurch implizit auf alle Websites der Webanwendung

berechtigt. Sie können auf einzelne Zonen eingeschränkt werden oder für alle Zonen der Webanwendung gelten.

SharePoint Berechtigungsrichtlinien

Auf dem Überblicksformular einer Berechtigungsrichtlinie werden die Webanwendung dargestellt sowie die Benutzerrichtlinien, denen die Berechtigungsrichtlinie zugewiesen ist. Es werden alle explizit erteilten und verweigerten Berechtigungen aufgelistet.

Um einen Überblick über eine Berechtigungsrichtlinie zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Berechtigungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Berechtigungsrichtlinie.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Berechtigungsrichtlinie**.

Für die Berechtigungsrichtlinie "Deny Write" wird als verweigerte Berechtigung die SharePoint Berechtigung "Deny Write" angezeigt. SharePoint fasst damit intern mehrere Einzelberechtigungen zusammen, die nur in der SharePoint Benutzeroberfläche in Einzelberechtigungen aufgelöst werden. Der One Identity Manager bildet die SharePoint-internen Berechtigungen ab. Dadurch erscheint in der One Identity Manager-Oberfläche nur die Berechtigung "Deny Write". Dem One Identity Manager sind die damit verbundenen Einzelberechtigungen nicht bekannt.

SharePoint Benutzerrichtlinien

Benutzerrichtlinien verfügen über einen dynamischen Fremdschlüssel (Spalte **Authentifizierungsobjekt**), der auf das jeweilige Authentifizierungsobjekt verweist. Verweist der dynamische Fremdschlüssel auf ein Active Directory oder LDAP Benutzerkonto, kann zusätzlich eine Person zugeordnet werden.

Jede Benutzerrichtlinie repräsentiert ein Objekt aus einem Authentifizierungssystem. Dieses Objekt kann eine Gruppe oder ein Benutzer sein.

Um die Stammdaten einer Benutzerrichtlinie zu bearbeiten

1. Wählen Sie die Kategorie **SharePoint | Benutzerrichtlinien**.
2. Wählen Sie in der Ergebnisliste die SharePoint Rolle. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Für Benutzerrichtlinien werden die folgenden Stammdaten abgebildet.

Tabelle 42: Stammdaten einer Benutzerrichtlinie

Eigenschaft	Beschreibung
Anzeigename	Anzeigename der Benutzerrichtlinie.
Benutzerkonto	Angabe, ob das Authentifizierungsobjekt der Benutzerrichtlinie ein Benutzerkonto ist.
Anmeldename	Anmeldename der Benutzerrichtlinie. Er wird über eine Bildungsregeln ermittelt.
Systemkonto	Angabe, ob die Benutzerrichtlinie in der SharePoint-Umgebung als Systemkonto geführt wird.
Person	Person, welche die Benutzerrichtlinie verwendet. Wenn ein Authentifizierungsobjekt zugeordnet ist, wird die verbundene Person per Bildungsregel über das Authentifizierungsobjekt ermittelt. Wenn kein Authentifizierungsobjekt zugeordnet ist, kann die Person manuell zugeordnet werden. Eine Person kann nur zugeordnet werden, wenn die Option **Benutzerkonto** aktiviert ist.
Webanwendung	Eindeutige Kennung der Webanwendung, für welche die Benutzerrichtlinie eingerichtet wurde.
Zone	Eindeutige Kennung der SharePoint Zone, für welche die Benutzerrichtlinie gültig ist.
Authentifizierungsobjekt	Authentifizierungsobjekt, welches die Benutzerrichtlinie referenziert. Jede Benutzerrichtlinie repräsentiert ein Objekt aus einem Authentifizierungssystem, dem die SharePoint-Installation vertraut. Wenn dieses Authentifizierungssystem als Zielsystem im One Identity Manager verwaltet wird, kann das zur Authentifizierung genutzte Objekt an der Benutzerrichtlinie als Authentifizierungsobjekt hinterlegt werden. Das Authentifizierungsobjekt wird bei der Synchronisation automatisch zugeordnet. Wenn die Option **Benutzerkonto** aktiviert ist, können folgende Authentifizierungsobjekte zugeordnet sein: • Active Directory Benutzerkonten • LDAP Benutzerkonten Wenn die Option **Benutzerkonto** deaktiviert ist, können folgende Authentifizierungsobjekte zugeordnet sein: • Active Directory Gruppen • LDAP Gruppen

HINWEIS: Wenn das Authentifizierungsobjekt, das einer SharePoint Benutzerrichtlinie zugeordnet ist, aus der One Identity Manager-Datenbank gelöscht wird, wird der Verweis

auf das Authentifizierungsobjekt von der Benutzerrichtlinie entfernt. Gegebenenfalls zugeordnete Personen bleiben zugeordnet.

Globale Benutzerrichtlinien

Globale Benutzerrichtlinien sind Benutzerrichtlinien, die für alle Zonen gültig sind. Sie werden in der Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | Globale Benutzerrichtlinien** abgebildet.

Zonenspezifische Benutzerrichtlinien

Zonenspezifische Benutzerrichtlinien sind Benutzerrichtlinien, die für eine einzelne Zone einer Webanwendung gültig sind. Sie werden in der Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | Zonenspezifische Benutzerrichtlinien | <Zone>**> abgebildet.

10

Berichte über SharePoint Websitesammlungen

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 SharePoint Farmen stehen folgende Berichte zur Verfügung.

HINWEIS: Abhängig von den vorhandenen Modulen können weitere Berichte zur Verfügung stehen.

Tabelle 43: Berichte für das Zielsystem

Bericht	Beschreibung
Übersicht aller Zuweisungen (Websitesammlung)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die in der ausgewählten Websitesammlung mindestens ein Benutzerkonto besitzen.
Übersicht aller Zuweisungen (Webanwendung)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die in der ausgewählten Webanwendung mindestens ein Benutzerkonto besitzen.
Übersicht aller Zuweisungen (Gruppe)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, welche die ausgewählte Gruppe besitzen.
Unverbundene Benutzerkonten anzeigen	Der Bericht zeigt alle Benutzerkonten der Websitesammlung, denen keine Person zugeordnet ist. Der Bericht enthält die zugeordneten Gruppen und die Risikoeinschätzung.
Personen mit mehreren Benutzerkonten anzeigen	Der Bericht zeigt alle Personen, die mehrere Benutzerkonten in der Websitesammlung besitzen. Der Bericht enthält eine Risikoeinschätzung.
Abweichende Systemberechtigungen anzeigen	Der Bericht enthält alle Gruppen der Websitesammlung, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager.
Ungenutzte Benutzerkonten anzeigen	Der Bericht enthält alle Benutzerkonten der Websitesammlung, die in den letzten Monaten nicht genutzt wurden.

Bericht	Beschreibung
Benutzerkonten mit einer überdurchschnittlichen Anzahl an Systemberechtigungen anzeigen	Der Bericht enthält alle Benutzerkonten der Websitesammlungen, die eine überdurchschnittliche Anzahl an Gruppen besitzen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager | Analyse Datenqualität**.

Übersicht aller Zuweisungen

Für einige Objekte, wie beispielsweise Berechtigungen, Complianceregeln oder Rollen wird der Bericht **Übersicht aller Zuweisungen** angezeigt. Der Bericht ermittelt alle Rollen, wie beispielsweise Abteilungen, Kostenstellen, Standorte, Geschäftsrollen und IT Shop Strukturen, in denen sich Personen befinden, die das gewählte Basisobjekt besitzen. Dabei werden sowohl direkte als auch indirekte Zuweisungen des Basisobjektes berücksichtigt.

Beispiele

- Wird der Bericht für eine Ressource erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Ressource besitzen.
- Wird der Bericht für eine Gruppe oder andere Systemberechtigung erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Gruppe oder Systemberechtigung besitzen.
- Wird der Bericht für eine Complianceregel erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Complianceregel verletzen.
- Wird der Bericht für eine Abteilung erstellt, werden alle Rollen ermittelt, in denen die Personen der gewählten Abteilung ebenfalls Mitglied sind.
- Wird der Bericht für eine Geschäftsrolle erstellt, werden alle Rollen ermittelt, in denen die Personen der gewählten Geschäftsrolle ebenfalls Mitglied sind.

Um detaillierte Informationen über Zuweisungen anzuzeigen

- Um den Bericht anzuzeigen, wählen Sie in der Navigation oder in der Ergebnisliste das Basisobjekt und wählen Sie den Bericht **Übersicht aller Zuweisungen**.
- Wählen Sie über die Schaltfläche **Verwendet von** in der Symbolleiste des Berichtes die Rollenklasse, für die Sie ermitteln möchten, ob es Rollen gibt, in denen sich Personen mit dem ausgewählten Basisobjekt befinden.

  Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Personen befinden, denen das ausgewählte Basisobjekt zugewiesen ist. Die Bedeutung der Steuerelemente des Berichts ist in einer separaten Legende erläutert. Die Legende erreichen Sie über das Symbol in der Symbolleiste des Berichtes.
- Mit einem Maus-Doppelklick auf das Steuerelement einer Rolle zeigen Sie alle untergeordneten Rollen der ausgewählten Rolle an.

- Mit einem einfachen Mausklick auf die Schaltfläche im Steuerelement einer Rolle zeigen Sie alle Personen dieser Rolle an, die das Basisobjekt besitzen.
- Über den Pfeil rechts neben der Schaltfläche starten Sie einen Assistenten, mit dem Sie die Liste der angezeigten Personen zur Nachverfolgung speichern können. Dabei wird eine neue Geschäftsrolle erstellt und die Personen werden der Geschäftsrolle zugeordnet.

Abbildung 6: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 44: Bedeutung der Symbole in der Symbolleiste des Berichts

Symbol	Bedeutung
	Anzeigen der Legende mit der Bedeutung der Steuerelemente des Berichts.
	Speichern der aktuellen Ansicht des Berichts als Bild.
	Auswählen der Rollenklasse, über die der Bericht erstellt werden soll.
	Anzeige aller Rollen oder Anzeige der betroffenen Rolle.

Anhang A

Konfigurationsparameter für die Verwaltung einer SharePoint-Umgebung

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

Tabelle 45: Konfigurationsparameter

Konfigurationsparameter	Beschreibung
TargetSystem\SharePoint	Der Bereich SharePoint wird unterstützt. Der Parameter ist ein präprozessorrelevanter Konfigurationsparameter. Die Aktivierung oder Deaktivierung des Konfigurationsparameters erfordert eine Kompilierung der Datenbank.
TargetSystem\SharePoint\Accounts	Parameter zur Konfiguration von SharePoint Benutzerkonten. Wenn der Parameter aktiviert ist, können die Einstellungen für SharePoint Benutzerkonten konfiguriert werden.
TargetSystem\SharePoint\Accounts\MailTemplateDefaultValues	Der Konfigurationsparameter enthält die Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei

Konfigurationsparameter	Beschreibung
	der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden.
TargetSystem\SharePoint\DBDeleteOnError	Schlägt das Anlegen eines Benutzerkontos im Zielsystem fehl, so wird das Objekt hinterher aus der Datenbank gelöscht.
TargetSystem\SharePoint\DefaultAddress	Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse für Benachrichtigungen, wenn im Zielsystem Aktionen fehlschlagen.
TargetSystem\SharePoint\MaxFullsyncDuration	Angabe der maximalen Laufzeit für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor.
TargetSystem\SharePoint\PersonAutoDefault	Anhand des angegebenen Modus erfolgt die automatische Personenzuordnung für Benutzerkonten, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem\SharePoint\PersonAutoFullsync	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.

Anhang B

Standardprojektvorlage für SharePoint

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.

Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 46: Abbildung der SharePoint Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im SharePoint	Tabelle im One Identity Manager Schema
SPAlternateUrl	SPSAlternateURL
SPClaimProvider	SPSClaimProvider
SPFarm	SPSFarm
SPGroup	SPSGroup
SPLanguage	SPSLanguage
SPPolicy	SPSPolicyUser
SPPolicyRole	SPSPolicyRole
SPPrefix	SPSPrefix
SPQuotaTemplate	SPSQuota
SPRoleDefinition	SPSRole
RoleAssignment	SPSRlAsgn

Schematyp im SharePoint	Tabelle im One Identity Manager Schema
SPSite	SPSSite
SPUser	SPSUser
SPWeb	SPSWeb
SPWebApplication	SPSWebApplication
SPWebTemplate	SPSWebTemplate

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

E

F

G

I

J

K

L

M

O

P

R

S

U

V

W

Z