One Identity Manager 8.2.1

Administrationshandbuch für die Anbindung einer SharePoint Online-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 Online-Umgebung
Aktualisiert - 27. April 2022, 02:56 Uhr
Version - 8.2.1

Inhalt

Abbilden einer SharePoint Online-Umgebung im One Identity Manager

Der One Identity Manager bietet eine vereinfachte Administration der Benutzer einer SharePoint Online-Umgebung. Dabei konzentriert sich der One Identity Manager auf die Abbildung von Websitesammlungen, Websites und Gruppen, die in einer Cloud-Umgebung liegen.

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

Durch die Datensynchronisation werden die Systeminformationen zur SharePoint Online Struktur in die One Identity Manager-Datenbank eingelesen. Aufgrund der komplexen Zusammenhänge und weitreichenden Auswirkungen von Änderungen ist die Anpassung dieser Systeminformationen im One Identity Manager nur bedingt möglich.

Ausführliche Information zur SharePoint Online Struktur finden Sie in der *SharePoint Online Dokumentation* von Microsoft.

Verwandte Themen

- Verarbeitung von Systemobjekten auf Seite 166

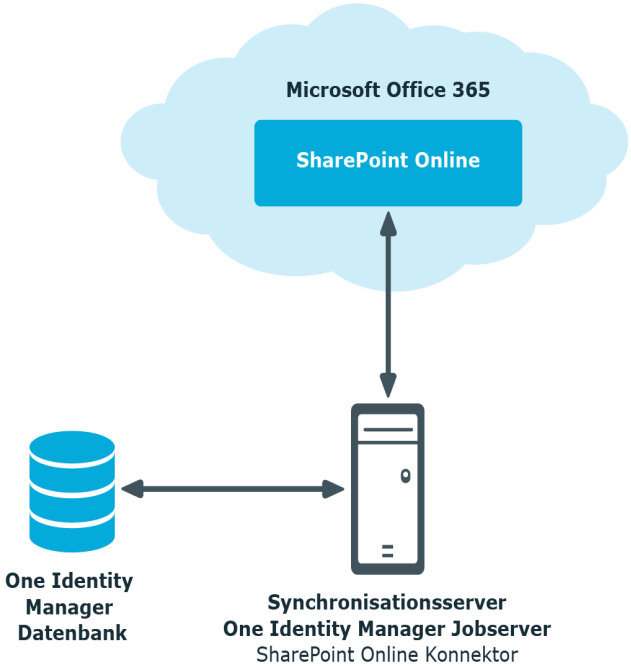
Architekturüberblick

Um auf die Daten eines SharePoint Online Mandanten zuzugreifen, wird auf einem Synchronisationsserver der SharePoint Online Konnektor installiert. Der Synchronisationsserver sorgt für den Abgleich der Daten zwischen der One Identity Manager-Datenbank und SharePoint Online. Der SharePoint Online Konnektor ist Bestandteil des SharePoint Online Moduls und verantwortlich für die Kommunikation mit dem SharePoint Online-Anteil des Microsoft Office 365 Abonnements in der Cloud. Die Microsoft CSOM (Client-side object model) Bibliothek wird für den Zugriff auf die SharePoint Online Daten verwendet.

HINWEIS: Für den Zugriff auf die Daten eines SharePoint Online Mandanten muss der Azure Active Directory Mandant, mit dem der SharePoint Online Mandant angebunden ist, synchronisiert werden.

Ausführliche Informationen zum Synchronisieren eines Azure Active Directory Mandanten finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung*.

Abbildung 1: Architektur für die Synchronisation



One Identity Manager Benutzer für die Verwaltung einer SharePoint Online-Umgebung

In die Einrichtung und Verwaltung einer SharePoint Online-Umgebung sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Zielsystemadministratoren	Die Zielsystemadministratoren müssen der Anwendungsrolle **Zielsysteme | Administratoren** zugewiesen sein.

Benutzer	Aufgaben
	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 Online** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische

Benutzer	Aufgaben
	Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen 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:
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 Servicekategorien, für die sie verantwortlich sind.
Administratoren für Organisationen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Organisationen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle:
Administratoren für Geschäftsrollen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Geschäftsrollen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle:

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 Online auf Seite 163.

2

Synchronisieren einer SharePoint Online-Umgebung

Der One Identity Manager unterstützt die Synchronisation mit SharePoint Online. Für den Abgleich der Informationen zwischen der One Identity Manager-Datenbank und der SharePoint Online-Umgebung sorgt der One Identity Manager Service.

Informieren Sie sich hier:

- wie Sie die Synchronisation einrichten, um initial Daten aus einem SharePoint Online Mandanten in die One Identity Manager-Datenbank einzulesen,
- wie Sie eine Synchronisationskonfiguration anpassen,
- wie Sie die Synchronisation starten und deaktivieren,
- wie Sie die Synchronisationsergebnisse auswerten.

TIPP: Bevor Sie die Synchronisation mit einem SharePoint Online Mandanten einrichten, machen Sie sich mit dem Synchronization Editor vertraut. Ausführliche Informationen über dieses Werkzeug finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Detaillierte Informationen zum Thema

- Einrichten der Initialsynchronisation mit einem SharePoint Online Mandanten auf Seite 14
- Anpassen einer Synchronisationskonfiguration auf Seite 31
- Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen auf Seite 30
- Ausführen einer Synchronisation auf Seite 40
- Fehleranalyse auf Seite 48
- Verarbeitung von Systemobjekten auf Seite 166

Einrichten der Initialsynchronisation mit einem SharePoint Online Mandanten

Der Synchronization Editor stellt eine Projektvorlage bereit, mit denen die Synchronisation von Benutzerkonten und Berechtigungen der SharePoint Online-Umgebung eingerichtet werden kann. Nutzen Sie diese Projektvorlagen, um Synchronisationsprojekte zu erstellen, mit denen Sie Daten aus einem SharePoint Online Mandanten in Ihre One Identity Manager-Datenbank einlesen. Zusätzlich werden die notwendigen Prozesse angelegt, über die Änderungen an Zielsystemobjekten aus der One Identity Manager-Datenbank in das Zielsystem provisioniert werden.

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

1. Stellen Sie im Azure Active Directory Mandanten ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit. Der Azure Active Directory Mandant muss im One Identity Manager bekannt sein.
2. Wenn Sie für die Anmeldung an SharePoint Online die Authentifizierung über eine Azure Active Directory Anwendung nutzen wollen, integrieren Sie den One Identity Manager als Anwendung in dem Azure Active Directory Mandanten, der mit Ihrem Office 365 Mandanten verknüpft ist.
    - Laden Sie die Zertifikatsdatei mit dem privaten Schlüssel (`*.PFX`) in den Zertifikatsspeicher des Synchronisationsservers und der administrativen Arbeitsstation, auf welcher der Synchronization Editor ausgeführt wird.
3. Die One Identity Manager Bestandteile für die Verwaltung von SharePoint Online-Umgebungen sind verfügbar, wenn der Konfigurationsparameter **TargetSystem | SharePointOnline** aktiviert ist.
    - Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.

      HINWEIS: Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
    - Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.
4. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
5. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Detaillierte Informationen zum Thema

- Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung auf Seite 15
- Integrieren des One Identity Manager als Anwendung im Azure Active Directory auf Seite 17
- Systemanforderungen für den SharePoint Online Synchronisationsserver auf Seite 18
- Vorbereiten der administrativen Arbeitsstation für den Zugriff auf SharePoint Online auf Seite 22
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines SharePoint Online Mandanten auf Seite 23
- Konfigurationsparameter für die Verwaltung einer SharePoint Online auf Seite 163
- Standardprojektvorlage für SharePoint Online auf Seite 165

Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung

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

Tabelle 2: Benutzer für die Synchronisation

Benutzer	Berechtigungen

Benutzer für den Zugriff auf SharePoint Online (Synchronisationsbenutzer)	Für eine vollständige Synchronisation von Objekten eines SharePoint Online Mandanten mit der ausgelieferten One Identity Manager Standardkonfiguration stellen Sie ein Benutzerkonto bereit, das die benötigten Mindestberechtigungen besitzt. Benötigt wird:
	• ein administratives Benutzerkonto des zugehörigen Azure Active Directory Mandanten, welches eine der folgenden Administratorrollen besitzt.
	  • SharePoint Administratoren
	  • Azure Active Directory Unternehmensadministrator/Globaler Administrator
	HINWEIS: Dieses Benutzerkonto muss an allen zu administrierenden Websitesammlungen als Websitesammlungsadministrator eingetragen werden. Dies nehmen Sie im SharePoint Online vor.

Benutzer	Berechtigungen
	Ausführliche Informationen zu Websitesammlungsadministratoren finden Sie in der Dokumentation von Microsoft.
Benutzerkonto des One Identity Manager Service	Das Benutzerkonto für den One Identity Manager Service benötigt die Benutzerrechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Verzeichnisse und Dateien anlegen und bearbeiten. Das Benutzerkonto muss der Gruppe **Domänen-Benutzer** angehören. Das Benutzerkonto benötigt das erweiterte Benutzerrecht **Anmelden als Dienst**. Das Benutzerkonto benötigt Berechtigungen 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 Berechtigungen 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) Für die Authentifizierung über eine Azure Active Directory Anwendung benötigt das Benutzerkonto im Zertifikatsspeicher des Computers das Zertifikat mit dem privaten Schlüssel (`*.PFX`-Datei). Das Zertifikat muss dasselbe Zertifikat sein, welches auch der Synchronisationsbenutzer verwendet.
Benutzer für den Zugriff auf die One Identity Manager-Datenbank	Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer **Synchronization** bereitgestellt.

Integrieren des One Identity Manager als Anwendung im Azure Active Directory

Um die Daten zwischen One Identity Manager und SharePoint Online zu synchronisieren, müssen Sie den One Identity Manager als Anwendung in dem Azure Active Directory Mandanten integrieren, der mit Ihrem Office 365 Mandanten verknüpft ist. Der SharePoint Online Konnektor authentifiziert sich über diese One Identity Manager Anwendung am Azure Active Directory Mandanten. Ausführliche Informationen zur Integration einer Unternehmensanwendung im Azure Active Directory finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung*.

HINWEIS: Beim Hinzufügen der One Identity Manager-Anwendung im Azure Active Directory wird eine Anwendungs-ID erzeugt. Die Anwendungs-ID benötigen Sie für die Einrichtung des Synchronisationsprojektes.

Ausführliche Informationen zum Registrieren einer Anwendung finden Sie unter https://docs.microsoft.com/de-de/azure/active-directory/develop/quickstart-register-app.

Um den One Identity Manager für SharePoint Online als Anwendung im Azure Active Directory zu konfigurieren

1. Erstellen Sie ein selbstsigniertes X.509-Zertifikat mit dem Typ **Serverauthentifizierung**, das zur Authentifizierung der Anwendung gegen Azure Active Directory verwendet wird.

   Ausführliche Informationen dazu finden Sie in der *SharePoint Online Dokumentation* von Microsoft.
2. Registrieren Sie eine neue Anwendung, wie im *One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung* beschrieben.
   - Wählen Sie die Option **Accounts in this organizational directory only**.
3. Kopieren Sie die Anwendungs-ID.
4. Laden Sie die Zertifikatsdatei (`*.CER`) und kopieren Sie sich den Fingerabdruck des Zertifikats.

   Der Fingerabdruck wird beim Einrichten des Synchronisationsprojekts benötigt.
5. Fügen Sie der Anwendung folgende Berechtigungen hinzu.
   - API Berechtigungen:
     - Microsoft-APIs > SharePoint
   - Anwendungsberechtigungen:
     - Sites.FullControl.All
     - TermStore.ReadWrite.All
     - User.ReadWrite.All
6. Erteilen Sie die Administrator-Zustimmung für diese Berechtigungen (**API permissions > Grant consent > Grant admin consent for > Yes**).

Verwandte Themen

- Initiales Synchronisationsprojekt für SharePoint Online erstellen auf Seite 25

Einrichten des SharePoint Online Synchronisationsservers

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

Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem SharePoint Online Konnektor installiert werden.

Wenn für die Anmeldung an SharePoint Online die Authentifizierung über eine Azure Active Directory Anwendung genutzt wird, benötigt der One Identity Manager Service im Zertifikatsspeicher des Computers das Zertifikat mit dem privaten Schlüssel (*.PFX-Datei).

Detaillierte Informationen zum Thema

- Systemanforderungen für den SharePoint Online Synchronisationsserver auf Seite 18
- One Identity Manager Service mit SharePoint Online Konnektor installieren auf Seite 19
- Integrieren des One Identity Manager als Anwendung im Azure Active Directory auf Seite 17

Systemanforderungen für den SharePoint Online Synchronisationsserver

Für die Einrichtung der Synchronisation mit einem SharePoint Online Mandanten muss ein Server zur Verfügung gestellt werden, auf dem die nachfolgend genannte Software installiert ist:

- Windows Betriebssystem

  Unterstützt werden die Versionen:

  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012

- Microsoft .NET Framework Version 4.7.2 oder höher

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.

One Identity Manager Service mit SharePoint Online Konnektor installieren

Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem SharePoint Online Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein.

Tabelle 3: Eigenschaften des Jobservers

Eigenschaft	Wert
Serverfunktion	SharePoint Online Konnektor
Maschinenrolle	Server | Jobserver | SharePoint Online

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

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

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

HINWEIS: Das Programm führt eine Remote-Installation des One Identity Manager Service aus. Eine lokale Installation des Dienstes ist mit diesem Programm nicht möglich.

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*.

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*.

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 Jobserver 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 Online**.
5. Auf der Seite **Serverfunktionen** wählen Sie **SharePoint Online 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:
    1. Wählen Sie **Prozessabholung > sqlprovider**
    2. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
    3. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
- Für eine Verbindung zum Anwendungsserver:
    1. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
    2. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
    3. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.
    4. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
    5. 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** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.
10. Wenn die Datenbank verschlüsselt ist, wählen Sie auf der Seite **Datenbankschlüsseldatei auswählen** die Datei mit dem privaten Schlüssel.
11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
    - **Computer**: Erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
    - **Dienstkonto**: Erfassen Sie die Angaben zum Benutzerkonto unter dem der One Identity Manager Service läuft. Erfassen Sie das Benutzerkonto, das Kennwort zum Benutzerkonto und die Kennwortwiederholung.

    Die Installation des Dienstes erfolgt mit dem Benutzerkonto, mit dem Sie an der administrativen Arbeitsstation angemeldet sind. Möchten Sie ein anderes Benutzerkonto für die Installation des Dienstes nutzen, können Sie dieses in den erweiterten Optionen eintragen. Angaben zum One Identity Manager Service können Sie ebenfalls über die erweiterten Optionen ändern, beispielsweise das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den One Identity Manager Service.
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.

Vorbereiten der administrativen Arbeitsstation für den Zugriff auf SharePoint Online

Um im Synchronization Editor die Synchronisation mit SharePoint Online zu konfigurieren, muss der One Identity Manager Daten direkt aus der SharePoint Online-Umgebung auslesen. Wenn für die Anmeldung an SharePoint Online die Authentifizierung über eine Azure Active Directory Anwendung genutzt wird, benötigt der an der administrativen Arbeitsstation angemeldete Benutzer im Zertifikatsspeicher des Computers das Zertifikat mit dem privaten Schlüssel (*.PFX-Datei). Das Zertifikat muss dasselbe Zertifikat sein, welches auch der Synchronisationsbenutzer verwendet.

Ist der direkte Zugriff von der Arbeitsstation nicht möglich, können Sie einen Remoteverbindungsserver einrichten.

Verwandte Themen

- Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung auf Seite 15
- Vorbereiten eines Remoteverbindungsservers für den Zugriff auf den SharePoint Online Mandanten auf Seite 22

Vorbereiten eines Remoteverbindungsservers für den Zugriff auf den SharePoint Online Mandanten

Um die Synchronisation mit einem Zielsystem zu konfigurieren, muss der One Identity Manager Daten aus dem Zielsystem auslesen. Dabei kommuniziert der One Identity Manager direkt mit dem Zielsystem. Mitunter ist der direkte Zugriff von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, nicht möglich, beispielsweise aufgrund der Firewall-Konfiguration oder weil die Arbeitsstation nicht die notwendigen Hard- oder Softwarevoraussetzungen erfüllt. Wenn der direkte Zugriff von der Arbeitsstation nicht möglich ist, kann eine Remoteverbindung eingerichtet werden.

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

Konfiguration des Remoteverbindungsservers:

- One Identity Manager Service ist gestartet
- **RemoteConnectPlugin** ist installiert
- SharePoint Online Konnektor ist installiert

Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt.

TIPP: Der Remoteverbindungsserver benötigt dieselbe Konfiguration (bezüglich der installierten Software sowie der Berechtigungen und des Zertifikates des Benutzerkontos) wie der Synchronisationsserver. Nutzen Sie den Synchronisationsserver gleichzeitig als Remoteverbindungsserver, indem Sie lediglich das **RemoteConnectPlugin** zusätzlich installieren.

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

Verwandte Themen

- Einrichten des SharePoint Online Synchronisationsservers auf Seite 18
- Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung auf Seite 15

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines SharePoint Online Mandanten

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

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

Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

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

Tabelle 4: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Bezeichnung der Basis-domäne	Bezeichnung der Azure Active Directory Basisdomäne ohne `.onmicrosoft.com`.
Authentifizierungsdaten zur Anmeldung an SharePoint Online	• Anwendungs-ID und Fingerabdruck des Zertifikats bei Authentifizierung über eine Azure Active Directory Anwendung - ODER - • Benutzername und Kennwort bei klassischer Authentifizierung Beispiel: `<Benutzername des Synchronisationsnutzers>@yourorganization.onmicrosoft.com` Stellen Sie ein Benutzerkonto mit ausreichend Berechtigungen bereit. Weitere Informationen finden Sie unter Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung auf Seite 15.
Synchronisationsserver für SharePoint Online	Vom Synchronisationsserver werden alle Aktionen des One Identity Manager Service gegen die Zielsystemumgebung ausgeführt. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet. Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem SharePoint Online Konnektor installiert sein. **Tabelle 5: Eigenschaften des Jobservers** Eigenschaft: Wert Serverfunktion: SharePoint Online Konnektor Maschinenrolle: Server | Jobserver | SharePoint Online Weitere Informationen finden Sie unter Einrichten des SharePoint Online Synchronisationsservers auf Seite 18.
Verbindungsdaten zur One Identity Manager-Datenbank	• Datenbankserver • Name der Datenbank • SQL Server Anmeldung und Kennwort

Angaben	Erläuterungen
	• Angabe, ob integrierte Windows-Authentifizierung verwendet wird Die Verwendung der integrierten Windows-Authentifizierung wird nicht empfohlen. Sollten Sie das Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
Remote-verbindungsserver	Weitere Informationen finden Sie unter Vorbereiten eines Remoteverbindungsservers für den Zugriff auf den SharePoint Online Mandanten auf Seite 22.

Initiales Synchronisationsprojekt für SharePoint Online erstellen

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

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

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

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

Um ein initiales Synchronisationsprojekt für einen SharePoint Online Mandanten einzurichten

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

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

2. Wählen Sie den Eintrag **Zielsystemtyp SharePoint Online** und klicken Sie **Starten**.

   Der Projektassistent des Synchronization Editors wird gestartet.

3. Auf der Seite **Systemzugriff** legen Sie fest, wie der One Identity Manager auf das Zielsystem zugreifen kann.

   - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, möglich, nehmen Sie keine Einstellungen vor.

- Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, nicht möglich, können Sie eine Remoteverbindung herstellen.

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

4. Auf der Seite **Verbindungsinformationen eingeben** erfassen Sie die Anmeldeinformationen für die Verbindung zu SharePoint Online.

   - **Basisdomäne**: Bezeichnung der Azure Active Directory Basisdomäne ohne `.onmicrosoft.com`.
   - **Authentifizierungstyp**: Art der Authentifizierung, die der SharePoint Online Konnektor bei der Anmeldung an SharePoint Online nutzen soll. Wählen Sie **Azure Active Directory Anwendung** oder **Klassisch**.

   Für die Authentifizierung über eine Azure Active Directory Anwendung erfassen Sie folgende Daten:

   - **Authentifizierungsendpunkt**: Wählen Sie den Authentifizierungsendpunkt der Azure Active Directory Anwendung.
   - **Anwendungs-ID**: Anwendungs-ID, die bei der Integration des One Identity Manager als Anwendung des Azure Active Directory Mandanten erzeugt wurde.
   - **Fingerabdruck des Zertifikats**: Fingerabdruck des Zertifikats, das bei der Integration des One Identity Manager als Anwendung des Azure Active Directory Mandanten erzeugt wurde.

   Für die klassische Authentifizierung erfassen Sie folgende Daten:

   - **Benutzername**: Vollqualifizierter Namen (FQDN) des Benutzerkontos zur Anmeldung an SharePoint Online in der Form `user@domain`.

     Beispiel:

     `<Benutzername des Synchronisationsnutzers>@youroranization.onmicrosoft.com`
   - **Kennwort**: Kennwort des Benutzerkontos.

5. Auf der letzten Seite des Systemverbindungsassistenten können Sie die Verbindungsdaten speichern.

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

6. 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.

7. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.
8. Auf der Seite **Zielsystemzugriff einschränken** legen Sie fest, wie der Systemzugriff erfolgen soll. Zur Auswahl stehen:

Tabelle 6: Zielsystemzugriff festlegen

Option	Bedeutung
Das Zielsystem soll nur eingelesen werden.	Gibt an, 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.	Gibt an, 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.

9. 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.

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

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

Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

HINWEIS:

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

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

- 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.

WICHTIG: Nachdem das Synchronisationsprojekt eingerichtet wurde, muss zwingend im Synchronization Editor der Scope im Zielsystem angepasst werden.

Der Scope darf nur die Websitesammlungen umfassen, in denen der verwendete Synchronisationsbenutzer in der SharePoint Online Administrationsoberfläche als Websitesammlungsadministrator eingetragen wurde. Es gibt keinen Standardbenutzer in der SharePoint Online-Umgebung.

Wenn der Scope nicht korrekt eingestellt ist, bricht die Synchronisation beim Laden der zu synchronisierenden Websitesammlungen ab.

Um Websitesammlungen im Scope eines SharePoint Online-Synchronisationsprojektes zu bearbeiten

1. Öffnen Sie den Synchronization Editor.
2. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
3. Wählen Sie die Ansicht **Scope**.
4. Klicken Sie **Scope bearbeiten**. Auf der rechten Seite erscheint eine Liste von Websitesammlungen.

5. Aktivieren Sie die zu synchronisierenden Websitesammlungen.

   Wählen Sie in der Liste der Websitesammlungen nur die, in denen der Synchronisationsbenutzer dem Administrator der SharePoint Online-Umgebung entspricht.
6. Klicken Sie **Übernahme in Datenbank**, um die Änderungen zu speichern.

Verwandte Themen

- Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung auf Seite 15
- Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen auf Seite 30
- Einrichten des SharePoint Online Synchronisationsservers auf Seite 18
- Synchronisationsprotokoll konfigurieren auf Seite 29
- Anpassen einer Synchronisationskonfiguration auf Seite 31
- Integrieren des One Identity Manager als Anwendung im Azure Active Directory auf Seite 17

Synchronisationsprotokoll konfigurieren

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

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

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

   - ODER -

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

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

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

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

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 42

Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen

Für die Synchronisation von SharePoint Online-Umgebungen gibt es einige Besonderheiten, die hier beschrieben werden.

- Es wird nur ein SharePoint Online Mandant pro Synchronisationsprojekt unterstützt. Zusätzliche Basisobjekte können nicht hinzugefügt werden.
- Das Zielsystemschema im One Identity Manager lässt sich nicht erweitern.
- Nachdem das Synchronisationsprojekt eingerichtet wurde, muss zwingend im Synchronization Editor der Scope im Zielsystem angepasst werden.

  Der Scope darf nur die Websitesammlungen umfassen, in denen der verwendete Synchronisationsbenutzer in der SharePoint Online Administrationsoberfläche als Websitesammlungsadministrator eingetragen wurde. Es gibt keinen Standardbenutzer in der SharePoint Online-Umgebung.

  Wenn der Scope nicht korrekt eingestellt ist, bricht die Synchronisation beim Laden der zu synchronisierenden Websitesammlungen ab.

  Um Websitesammlungen im Scope eines SharePoint Online-Synchronisationsprojektes zu bearbeiten

  1. Öffnen Sie den Synchronization Editor.
  2. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
  3. Wählen Sie die Ansicht **Scope**.
  4. Klicken Sie **Scope bearbeiten**. Auf der rechten Seite erscheint eine Liste von Websitesammlungen.
  5. Aktivieren Sie die zu synchronisierenden Websitesammlungen.

     Wählen Sie in der Liste der Websitesammlungen nur die, in denen der Synchronisationsbenutzer dem Administrator der SharePoint Online-Umgebung entspricht.
  6. Klicken Sie **Übernahme in Datenbank**, um die Änderungen zu speichern.

Verwandte Themen

- Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung auf Seite 15
- Synchronisationsfehler nach Umbenennung einer SharePoint Online Websitesammlung auf Seite 162

Anpassen einer Synchronisationskonfiguration

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation eines SharePoint Online Mandanten eingerichtet. Mit diesem Synchronisationsprojekt können Sie SharePoint Online Websitesammlungen in die One Identity Manager-Datenbank einlesen. Wenn Sie Websites, Benutzer und Gruppen mit dem One Identity Manager verwalten, werden Änderungen in den SharePoint Online Mandanten provisioniert.

Um die One Identity Manager-Datenbank und den SharePoint Online Mandanten regelmäßig abzugleichen und Änderungen zu synchronisieren, passen Sie die Synchronisationskonfiguration an.

- Um bei der Synchronisation den One Identity Manager als primäres System zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um festzulegen, welche SharePoint Online Objekte und One Identity Manager-Datenbankobjekte bei der Synchronisation behandelt werden, bearbeiten Sie den Scope der Zielsystemverbindung und der One Identity Manager-Datenbankverbindung. Um Dateninkonsistenzen zu vermeiden, definieren Sie in beiden Systemen den gleichen Scope. Ist kein Scope definiert, werden alle Objekte synchronisiert.
- Um allgemeingültige Synchronisationskonfigurationen zu erstellen, die erst beim Start der Synchronisation die notwendigen Informationen über die zu synchronisierenden Objekte erhalten, können Variablen eingesetzt werden. Variablen können beispielsweise in den Basisobjekten, den Schemaklassen oder den Verarbeitungsmethoden eingesetzt werden.
- Wenn sich das One Identity Manager Schema oder das Zielsystemschema geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.
- Um zusätzliche Schemaeigenschaften zu synchronisieren, aktualisieren Sie das Schema im Synchronisationsprojekt. Nehmen Sie die Schemaerweiterungen in das Mapping auf.

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

Detaillierte Informationen zum Thema

- Synchronisation in den SharePoint Online Mandanten konfigurieren auf Seite 32
- Einstellungen der Systemverbindung zum SharePoint Online Mandanten ändern auf Seite 32
- Schema aktualisieren auf Seite 35
- Provisionierung von Mitgliedschaften konfigurieren auf Seite 36
- Einzelobjektsynchronisation konfigurieren auf Seite 38
- Beschleunigung der Provisionierung und Einzelobjektsynchronisation auf Seite 39

Synchronisation in den SharePoint Online Mandanten 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 primäres System zu nutzen, benötigen Sie zusätzlich einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.

Um eine Synchronisationskonfiguration für die Synchronisation in die SharePoint Online-Umgebung zu erstellen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
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.

Einstellungen der Systemverbindung zum SharePoint Online Mandanten ändern

Beim Einrichten der initialen Synchronisation werden für die Eigenschaften der Systemverbindung Standardwerte gesetzt. Diese Standardwerte können angepasst werden. Dafür gibt es zwei Wege:

a. Legen Sie ein spezialisiertes Variablenset an und ändern Sie die Werte der betroffenen Variablen.

   Die Standardwerte bleiben im Standardvariablenset erhalten. Die Variablen können jederzeit auf die Standardwerte zurückgesetzt werden. (Empfohlenes Vorgehen)

b. Bearbeiten Sie die Zielsystemverbindung mit dem Systemverbindungsassistenten und ändern Sie die betroffenen Werte.

   Der Systemverbindungsassistent liefert zusätzliche Erläuterungen zu den Einstellungen. Die Standardwerte können nur unter bestimmten Voraussetzungen wiederhergestellt werden.

Detaillierte Informationen zum Thema

- Verbindungsparameter im Variablenset bearbeiten auf Seite 33
- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 34

Verbindungsparameter im Variablenset bearbeiten

Die Verbindungsparameter wurden beim Einrichten der Synchronisation als Variablen im Standardvariablenset gespeichert. Sie können die Werte dieser Variablen in einem spezialisierten Variablenset Ihren Erfordernissen anpassen und dieses Variablenset einer Startkonfiguration und einem Basisobjekt zuordnen. Damit haben Sie jederzeit die Möglichkeit, erneut die Standardwerte aus dem Standardvariablenset zu nutzen.

HINWEIS: Um die Datenkonsistenz in den angebundenen Zielsystemen zu bewahren, stellen Sie sicher, dass die Startkonfiguration für die Synchronisation und das Basisobjekt für die Provisionierung dasselbe Variablenset verwenden.

Um die Verbindungsparameter in einem spezialisierten Variablenset anzupassen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
3. Öffnen Sie die Ansicht **Verbindungsparameter**.

   Einige Verbindungsparameter können hier in Variablen umgewandelt werden. Für andere sind bereits Variablen angelegt.
4. Wählen Sie einen Parameter und klicken Sie **Umwandeln**.
5. Wählen Sie die Kategorie **Konfiguration > Variablen**.

   Im unteren Bereich der Dokumentenansicht werden alle spezialisierten Variablensets angezeigt.
6. Wählen Sie ein spezialisiertes Variablenset oder klicken Sie in der Symbolleiste der Variablensetansicht .

- Um das Variablenset umzubenennen, markieren Sie das Variablenset und klicken Sie in der Symbolleiste der Variablensetansicht . Erfassen Sie einen Namen für das Variablenset.

7. Wählen Sie die zuvor angelegten Variablen und erfassen Sie neue Werte.
8. Wählen Sie die Kategorie **Konfiguration > Startkonfigurationen**.
9. Wählen Sie eine Startkonfiguration und klicken Sie **Bearbeiten**.
10. Wählen Sie den Tabreiter **Allgemein**.
11. Ordnen Sie im Eingabefeld **Variablenset** das spezialisierte Variablenset zu.
12. Wählen Sie die Kategorie **Konfiguration > Basisobjekte**.
13. Wählen Sie ein Basisobjekt und klicken Sie .

    - ODER -

    Klicken Sie , um ein neues Basisobjekt anzulegen.
14. Ordnen Sie im Eingabefeld **Variablenset** das spezialisierte Variablenset zu.
15. Speichern Sie die Änderungen.

Ausführliche Informationen zur Anwendung von Variablen und Variablensets, zum Wiederherstellen der Standardwerte und zum Anlegen von Basisobjekten finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 34

Eigenschaften der Zielsystemverbindung bearbeiten

Die Verbindungsparameter können auch mit dem Systemverbindungsassistenten geändert werden. Wenn für die Einstellungen Variablen definiert sind, werden die Änderungen in das aktive Variablenset übernommen.

HINWEIS: Unter folgenden Umständen können die Standardwerte nicht wiederhergestellt werden:

- Die Verbindungsparameter sind nicht als Variablen hinterlegt.
- Das Standardvariablenset ist als aktives Variablenset ausgewählt.

In beiden Fällen überschreibt der Systemverbindungsassistent die Standardwerte. Sie können später nicht wiederhergestellt werden.

Um die Verbindungsparameter mit dem Systemverbindungsassistenten zu bearbeiten

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie in der Symbolleiste das aktive Variablenset, das für die Verbindung zum Zielsystem verwendet werden soll.

   HINWEIS: Ist das Standardvariablenset ausgewählt, werden die Standardwerte überschrieben und können später nicht wiederhergestellt werden.
3. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
4. Klicken Sie **Verbindung bearbeiten**.

   Der Systemverbindungsassistent wird gestartet.
5. Folgen Sie den Anweisungen des Systemverbindungsassistenten und ändern Sie die gewünschten Eigenschaften.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Verbindungsparameter im Variablenset bearbeiten auf Seite 33

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 im Synchronization Editor das Synchronisationsprojekt.
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 im Synchronization Editor das Synchronisationsprojekt.
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.

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 `Members` einer SharePoint Online Gruppe (`Group`)
- 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 Online > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **SharePoint Online**.
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.
5. Klicken Sie **Merge-Modus**.

   HINWEIS:

   - 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.
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. Dabei werden nur die neu eingefügten und gelöschten Zuordnungen verarbeitet. 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 Symbol gekennzeichnet:  . Die originale Bedingung kann jederzeit wiederhergestellt werden.

Um die originale Bedingung 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.

HINWEIS: Um in der Bedingung den Bezug zu den eingefügten oder gelöschten Zuordnungen herzustellen, nutzen Sie den Tabellenalias `i`.

Beispiel für eine Bedingung an der Zuordnungstabelle `O3SUserInGroup`:

```
exists (select top 1 1 from O3SGroup g
      where g.UID_O3SGroup = i.UID_O3SGroup
      and <einschränkende Bedingung>)
```

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

Einzelobjektsynchronisation konfigurieren

Änderungen an einem einzelnen Objekt im Zielsystem können sofort in die One Identity Manager-Datenbank übertragen werden, ohne dass eine vollständige Synchronisation der Zielsystem-Umgebung gestartet werden muss. Die Einzelobjektsynchronisation kann nur für Objekte ausgeführt werden, die in der One Identity Manager-Datenbank bereits vorhanden sind. Es werden die Änderungen an den gemappten Objekteigenschaften übernommen. Gehört zu diesen Objekteigenschaften eine Mitgliederliste, werden auch die Einträge in der Zuordnungstabelle aktualisiert. Ist das Objekt im Zielsystem nicht mehr vorhanden, wird es in der One Identity Manager-Datenbank gelöscht.

Voraussetzungen

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

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

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

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **SharePoint Online**.
3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die kundenspezifische Tabelle zu, für die Sie die Einzelobjektsynchronisation nutzen möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die kundenspezifische Tabelle und erfassen Sie den **Pfad zum Basisobjekt**.

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

   Beispiel: `FK(UID_O3STenant).XObjectKey`
8. Speichern Sie die Änderungen.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 43
- Ausstehende Objekte nachbehandeln auf Seite 45

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.
   - Für Jobserver, die an der Lastverteilung teilnehmen, muss die Option **Keine Prozesszuteilung** deaktiviert sein.
   - Weisen Sie diesen Jobservern die Serverfunktion **SharePoint Online Konnektor** zu.

   Alle Jobserver müssen auf den gleichen SharePoint Online Mandanten zugreifen können, wie der Synchronisationsserver für das jeweilige Basisobjekt.

2. Weisen Sie im Synchronization Editor an das Basisobjekt eine kundendefinierte Serverfunktion zu.

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

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

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

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

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

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

Um den Synchronisationsserver ohne Lastverteilung zu nutzen

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

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

Detaillierte Informationen zum Thema

- Server bearbeiten

Ausführen einer Synchronisation

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

Bevor Sie eine Synchronisation der SharePoint Online-Umgebung ausführen, muss die Azure Active Directory-Umgebung in One Identity Manager auf dem aktuellsten Stand sein.

> HINWEIS: Führen Sie regelmäßige Synchronisationen der Azure Active Directory-Umgebung aus. Die folgende Synchronisationsreihenfolge ist zwingend einzuhalten:
>
> 1. Azure Active Directory
> 2. SharePoint Online

Wenn verschiedene Zielsysteme immer in einer vorher festgelegten Reihenfolge synchronisiert werden sollen, nutzen Sie Startfolgen, um die Synchronisation zu starten. In

einer Startfolge können beliebige Startkonfigurationen aus verschiedenen Synchronisationsprojekten zusammengestellt und in eine Ausführungsreihenfolge gebracht werden. Ausführliche Informationen zu Startfolgen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Detaillierte Informationen zum Thema

- Synchronisationen starten auf Seite 41
- Synchronisation deaktivieren auf Seite 43
- Synchronisationsergebnisse anzeigen auf Seite 42

Synchronisationen starten

Beim Einrichten des initialen Synchronisationsprojekts über das Launchpad werden Standardzeitpläne für regelmäßige Synchronisationen erstellt und zugeordnet. Um regelmäßige Synchronisationen auszuführen, aktivieren Sie diese Zeitpläne.

Um regelmäßige Synchronisationen auszuführen

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

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

Um die initiale Synchronisation manuell zu starten

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

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

- Wenn eine weitere Synchronisation mit derselben Startkonfiguration gestartet wird, wird dieser Prozess gestoppt und erhält den Ausführungsstatus **Frozen**. Es wird eine Fehlermeldung in die Protokolldatei des One Identity Manager Service

geschrieben.

- Stellen Sie sicher, dass Startkonfigurationen, die in Startfolgen verwendet werden, nicht gleichzeitig einzeln gestartet werden. Weisen Sie den Startfolgen und Startkonfigurationen unterschiedliche Zeitpläne zu.

- Wenn eine weitere Synchronisation mit einer anderen Startkonfiguration gestartet wird, die dasselbe Zielsystem anspricht, kann das zu Synchronisationsfehlern oder Datenverlust führen. Legen Sie an den Startkonfigurationen fest, wie sich der One Identity Manager in diesem Fall verhalten soll.
  - Stellen Sie über den Zeitplan sicher, dass die Startkonfigurationen nacheinander ausgeführt werden.
  - Gruppieren Sie die Startkonfigurationen mit gleichem Startverhalten.

Synchronisationsergebnisse anzeigen

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

Um das Protokoll einer Synchronisation anzuzeigen

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

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

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

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

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

Verwandte Themen

- Synchronisationsprotokoll konfigurieren auf Seite 29
- Fehleranalyse auf Seite 48

Synchronisation deaktivieren

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

Um regelmäßige Synchronisationen zu verhindern

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

Einzelobjekte synchronisieren

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

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

Um ein Einzelobjekt zu synchronisieren

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

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

Besonderheiten bei der Synchronisation von Mitgliederlisten

Wenn Sie Änderungen in der Mitgliederliste eines Objekts synchronisieren, führen Sie die Einzelobjektsynchronisation am Basisobjekt der Zuweisung aus. Die Basistabelle einer Zuordnung enthält eine Spalte `XDateSubItem` mit der Information über die letzte Änderung der Mitgliedschaften.

Beispiel:

Basisobjekt für die Zuweisung von SharePoint Online Benutzerkonten an SharePoint Online Gruppen ist die Gruppe.

Im Zielsystem wurde ein Benutzerkonto an eine Gruppe zugewiesen. Um diese Zuweisung zu synchronisieren, wählen Sie im Manager die Gruppe, der das Benutzerkonto zugewiesen wurde, und führen Sie die Einzelobjektsynchronisation aus. Dabei werden alle Mitgliedschaften für diese Gruppe synchronisiert.

Das Benutzerkonto muss in der One Identity Manager-Datenbank bereits als Objekt vorhanden sein, damit die Zuweisung angelegt werden kann.

Detaillierte Informationen zum Thema

- Einzelobjektsynchronisation konfigurieren auf Seite 38

Aufgaben nach einer Synchronisation

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

- Ausstehende Objekte nachbehandeln auf Seite 45
- Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen auf Seite 47
- Benutzerkonten über Kontendefinitionen verwalten auf Seite 47

Ausstehende Objekte nachbehandeln

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 Online > Zielsystemabgleich: SharePoint Online**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp **SharePoint Online** 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

1. Wählen Sie auf dem Formular für den Zielsystemabgleich das Objekt.
2. 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 7: 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. Indirekte Mitgliedschaften können nicht gelöscht werden.
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung **Ausstehend** wird für das Objekt entfernt. Es 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 das Symbol  .

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

werden deaktiviert.

Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen

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

Um kundenspezifische Tabellen in den Zielsystemabgleich aufzunehmen

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

Verwandte Themen

- Ausstehende Objekte nachbehandeln auf Seite 45

Benutzerkonten über Kontendefinitionen verwalten

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.

Detaillierte Informationen zum Thema

- Kontendefinitionen an verbundene SharePoint Online Benutzerkonten zuweisen auf Seite 78

Fehleranalyse

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

- Synchronisation simulieren

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

- Synchronisation analysieren

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

- Meldungen protokollieren

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

- Startinformation zurücksetzen

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

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

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 42
- Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen auf Seite 30

Datenfehler bei der Synchronisation ignorieren

Standardmäßig werden Objekte mit fehlerhaften Daten nicht synchronisiert. Diese Objekte können synchronisiert werden, sobald die fehlerhaften Daten korrigiert wurden. In

einzelnen Situationen kann es notwendig sein, solche Objekte dennoch zu synchronisieren und nur die fehlerhaften Objekteigenschaften zu ignorieren. Dieses Verhalten kann für die Synchronisation in den One Identity Manager konfiguriert werden.

Um Datenfehler bei der Synchronisation in den One Identity Manager zu ignorieren

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > One Identity Manager Verbindung**.
3. In der Ansicht **Allgemein** klicken Sie **Verbindung bearbeiten**.

   Der Systemverbindungsassistent wird gestartet.
4. Auf der Seite **Weitere Einstellungen** aktivieren Sie **Versuche Datenfehler zu ignorieren**.

   Diese Option ist nur wirksam, wenn am Synchronisationsworkflow **Bei Fehler fortsetzen** eingestellt ist.

   Fehler in Standardspalten, wie Primärschlüssel oder UID-Spalten, und Pflichteingabespalten können nicht ignoriert werden.
5. Speichern Sie die Änderungen.

WICHTIG: Wenn die Option aktiviert ist, versucht der One Identity Manager Speicherfehler zu ignorieren, die auf Datenfehler in einer einzelnen Spalte zurückgeführt werden können. Dabei wird die Datenänderung an der betroffenen Spalte verworfen und das Objekt anschließend neu gespeichert. Das beeinträchtigt die Performance und führt zu Datenverlust.

Aktivieren Sie die Option nur im Ausnahmefall, wenn eine Korrektur der fehlerhaften Daten vor der Synchronisation nicht möglich ist.

3

Managen von SharePoint Online Benutzerkonten und Personen

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

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

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

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

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

Verwandte Themen

- Kontendefinitionen für SharePoint Online Benutzerkonten auf Seite 51
- Automatische Zuordnung von Personen zu SharePoint Online Benutzerkonten auf Seite 73
- SharePoint Online Benutzerkonten auf Seite 113

Kontendefinitionen für SharePoint Online Benutzerkonten

Um 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. 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.

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

Ausführliche Informationen zu den Grundlagen zu Kontendefinitionen, Automatisierungsgraden und zur Ermittlung der gültigen IT Betriebsdaten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

- Erstellen von Kontendefinitionen
- Konfigurieren der Automatisierungsgrade
- Erstellen der Abbildungsvorschriften für die IT Betriebsdaten

- Erfassen der IT Betriebsdaten
- Zuweisen der Kontendefinitionen an Personen und Zielsysteme

Detaillierte Informationen zum Thema

- Kontendefinitionen erstellen auf Seite 52
- Automatisierungsgrade bearbeiten auf Seite 56
- Abbildungsvorschriften für IT Betriebsdaten erstellen auf Seite 59
- IT Betriebsdaten erfassen auf Seite 61
- Zuweisen der Kontendefinition an Personen auf Seite 63
- Kontendefinitionen an SharePoint Online Websitesammlungen zuweisen auf Seite 69

Kontendefinitionen erstellen

Um eine Kontendefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular erfassen Sie die Stammdaten der Kontendefinition.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Kontendefinitionen auf Seite 53
- Kontendefinitionen bearbeiten auf Seite 52
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 57

Kontendefinitionen bearbeiten

Um eine Kontendefinition zu bearbeiten

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten der Kontendefinition.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Kontendefinitionen auf Seite 53
- Kontendefinitionen erstellen auf Seite 52
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 57

Stammdaten für Kontendefinitionen

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 8: 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	Angabe der vorausgesetzten Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch zugeordnet. TIPP: Sie können hier die Kontendefinition des zugehörigen Azure Active Directory Mandanten eintragen. In diesem Fall wird für die Person zunächst ein Azure Active Directory Benutzerkonto erzeugt. Ist dieses Benutzerkonto vorhanden, wird das SharePoint Online Benutzerkonto angelegt.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatisierungsgrad (initial)	Standardautomatisierungsgrad, der bei Neuanlage von Benutzerkonten standardmäßig verwendet werden soll.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Kontendefinition an Personen. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Leistungsposition	Leistungsposition, über welche die Kontendefinition im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue

Eigenschaft	Beschreibung
	Leistungsposition an.
IT Shop	Gibt an, 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	Gibt an, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren 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	Gibt an, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Um die Kontendefinition automatisch an alle internen Personen zuzuweisen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Personen aktivieren**. Die Kontendefinition wird an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine neue interne Person erstellt wird, erhält diese Person ebenfalls automatisch diese Kontendefinition. Um die automatische Zuweisung der Kontendefinition von allen Personen zu entfernen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Personen deaktivieren**. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.
Kontendefinition bei dauerhafter Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) 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: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.

Eigenschaft	Beschreibung
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: (Standard) 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: (Standard) 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.
Gruppen erbbar	Gibt an, ob das Benutzerkonto Gruppen über die verbundene Person erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Person Mitglied ist, oder über 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.
Rollen erbbar	Gibt an, ob das Benutzerkonto SharePoint Online Rollen über die verbundene Person erben darf. Ist die Option aktiviert, werden SharePoint Online Rollen über hierarchische Rollen, in denen die Person Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt.

Automatisierungsgrade bearbeiten

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 einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Kontendefinitionen > Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

4. Bearbeiten Sie die Stammdaten des Automatisierungsgrades.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Automatisierungsgrad auf Seite 58
- IT Betriebsdaten erfassen auf Seite 61
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 57

Automatisierungsgrade erstellen

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade **Unmanaged** und **Full managed**. Abhängig von Ihren Anforderungen können Sie weitere Automatisierungsgrade definieren.

WICHTIG: Erweitern Sie im Designer die Bildungsregeln um die Vorgehensweise für die zusätzlichen Automatisierungsgrade. Ausführliche Informationen zu Bildungsregeln finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um einen Automatisierungsgrad zu erstellen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Kontendefinitionen > Automatisierungsgrade**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten des Automatisierungsgrades.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Kontendefinitionen auf Seite 53
- Kontendefinitionen bearbeiten auf Seite 52
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 57

Automatisierungsgrade an Kontendefinitionen zuweisen

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

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > 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.

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

   Um eine Zuweisung zu entfernen

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

Stammdaten für Automatisierungsgrad

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 9: Stammdaten eines Automatisierungsgrades

Eigenschaft	Beschreibung
Automatisierungsgrad	Bezeichnung des Automatisierungsgrades.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Betriebsdaten überschreibend	Gibt an, ob Daten an Benutzerkonten, die sich aus den IT Betriebsdaten bilden, automatisch aktualisiert werden. Zulässige Werte sind: • **Niemals**: Die Daten werden nicht aktualisiert. (Standard) • **Immer**: Die Daten werden immer aktualisiert. • **Nur initial**: Die Daten werden nur initial ermittelt.
Gruppen bei zeitweiliger Deaktivierung beibehalten	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei zeitweiliger Deaktivierung sperren *)	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Personen gesperrt werden sollen.
Gruppen bei dauerhafter Deaktivierung beibehalten	Gibt an, ob die Benutzerkonten dauerhaft deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.

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

HINWEIS:*) SharePoint Online Benutzerkonten können nicht gesperrt werden!

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

Abbildungsvorschriften für IT Betriebsdaten erstellen

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

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

- SharePoint Online Authentifizierungsmodus
- Gruppen erbbar
- Rollen erbbar
- Privilegiertes Benutzerkonto

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **IT Betriebsdaten Abbildungsvorschrift bearbeiten.**
4. Klicken Sie **Hinzufügen** und erfassen Sie folgende Informationen.
   - **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.
   - **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: Die Geschäftsrolle kann nur verwendet werden, 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**: Gibt an, 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**: Gibt an, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkontos mit Standardwerten** verwendet.

     Um die Mailvorlage zu ändern, passen Sie im Designer den Konfigurationsparameter **TargetSystem | SharePoint Online | Accounts | MailTemplateDefaultValues** an.
5. Speichern Sie die Änderungen.

IT Betriebsdaten erfassen

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

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

Beispiel:

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

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

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

Um IT Betriebsdaten festzulegen

1. Wählen Sie im Manager in der Kategorie **Organisationen** oder **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten**.
3. Klicken Sie **Hinzufügen** und erfassen Sie die folgenden Daten.
    - **Wirksam für**: Legen Sie den Anwendungsbereich der IT Betriebsdaten fest. 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**: Wählen Sie die 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.

- **Wert**: Erfassen Sie den konkreten Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Abbildungsvorschriften für IT Betriebsdaten erstellen auf Seite 59

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, zu einer primären Geschäftsrolle oder zu einem primären Standort, werden die Bildungsregeln automatisch ausgeführt.

Um die Bildungsregeln auszuführen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > 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. Es bedeuten:

   - **Alter Wert**: Wert der Objekteigenschaft vor der Änderung der IT Betriebsdaten.
   - **Neuer Wert**: Wert der Objekteigenschaft nach der Änderung der IT Betriebsdaten.
   - **Auswahl**: Gibt an, ob der neue Wert 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.

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.

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.

Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

1. Wählen Sie im Manager in der Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.

   - ODER -

   Wählen Sie im Manager in der Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.
2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
   - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
   - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
3. Speichern Sie die Änderungen.

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

Detaillierte Informationen zum Thema

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 65
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 65
- Kontendefinitionen an alle Personen zuweisen auf Seite 66
- Kontendefinitionen direkt an Personen zuweisen auf Seite 66
- Kontendefinitionen an Systemrollen zuweisen auf Seite 67
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 67

Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

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

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

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

Kontendefinitionen an Geschäftsrollen zuweisen

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

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

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

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

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

Kontendefinitionen an alle Personen zuweisen

Über diese Aufgaben wird die Kontendefinition an alle internen Personen zugewiesen. Personen, die als externe Personen gekennzeichnet sind, erhalten die Kontendefinition nicht. Sobald eine neue interne Person erstellt wird, erhält diese Person ebenfalls automatisch diese Kontendefinition. Die Zuweisung wird durch den DBQueue Prozessor berechnet.

WICHTIG: Führen Sie die Aufgabe nur aus, 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 eine Kontendefinition an alle Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Automatische Zuweisung zu Personen aktivieren**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Speichern Sie die Änderungen.

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

Kontendefinitionen direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

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

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

   Um eine Zuweisung zu entfernen

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

Kontendefinitionen an Systemrollen zuweisen

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

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 Online > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Kontendefinitionen in den IT Shop aufnehmen

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

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

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

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

Um eine Kontendefinition in den IT Shop aufzunehmen (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
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 in den IT Shop aufzunehmen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
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 (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
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 einzelnen Regalen des IT Shops zu entfernen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
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 (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
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.

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
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 für Kontendefinitionen auf Seite 53

Kontendefinitionen an SharePoint Online Websitesammlungen zuweisen

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

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

Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand **Linked**). 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 Online > 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.

Verwandte Themen

- Automatische Zuordnung von Personen zu SharePoint Online Benutzerkonten auf Seite 73

Kontendefinitionen löschen

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

Um eine Kontendefinition zu löschen

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Personen.
    a. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Wählen Sie die Aufgabe **Automatische Zuweisung zu Personen deaktivieren**.
    e. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
    f. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Personen.
    a. Wählen Sie im Manager die Kategorie **SharePoint Online > 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 Online > 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 Online > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

   c. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.

   d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.

   e. Speichern Sie die Änderungen.

5. Entfernen Sie die Zuordnung der Kontendefinition zu IT Betriebsdaten.

   a. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

   c. Wählen Sie die Aufgabe **IT Betriebsdaten Abbildungsvorschrift bearbeiten**.

   d. Wählen Sie eine Spalte und klicken Sie **Entfernen**, um die Abbildungsvorschrift entfernen.

   e. Entfernen Sie alle Abbildungsvorschriften.

   f. Speichern Sie die Änderungen.

6. 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 Web Designer Web Portal Anwenderhandbuch*.

   Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen (bei rollenbasierter Anmeldung)

   a. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.

   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.

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen (bei nicht-rollenbasierter Anmeldung)

a. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

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.

7. 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 Online > 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.

8. Entfernen Sie die Zuordnung der Kontendefinition zum Zielsystem.

a. Wählen Sie im Manager in der Kategorie **SharePoint Online > 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.

9. Löschen Sie die Kontendefinition.

a. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

c. Klicken Sie , um die Kontendefinition zu löschen.

Automatische Zuordnung von Personen zu SharePoint Online Benutzerkonten

Beim Einfügen eines Benutzerkontos kann automatisch eine vorhandene Person zugeordnet werden. Dieser Mechanismus kann auf die Erstellung eines neuen Benutzerkontos durch manuelle Anlage oder Synchronisation folgen.Nach der Synchronisation werden automatisch an alle neuen Benutzerkonten Identitäten zugeordnet. Wenn keine passende Identität gefunden werden kann, wird eine neue Identität anhand vorhandener Benutzerstammdaten erzeugt.

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.

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

Voraussetzungen

- Bei den Benutzerkonten handelt es sich um Prinzipale vom Typ **Benutzer**.
- 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 | SharePointOnline | PersonAutoFullsync** und wählen Sie den gewünschten Modus.

- Wenn Personen außerhalb der Synchronisation zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | SharePointOnline | PersonAutoDefault** und wählen Sie den gewünschte Modus.
- 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.

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.

Weitere Informationen finden Sie unter Benutzerkonten über Kontendefinitionen verwalten auf Seite 47.

Verwandte Themen

- Kontendefinitionen erstellen auf Seite 52
- Kontendefinitionen an SharePoint Online Websitesammlungen zuweisen auf Seite 69
- Automatisierungsgrade für SharePoint Online Benutzerkonten ändern auf Seite 76
- Suchkriterien für die automatische Personenzuordnung bearbeiten auf Seite 74

Suchkriterien für die automatische Personenzuordnung bearbeiten

Die Kriterien für die Personenzuordnung werden an der Websitesammlung definiert. 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 `O3SSite` geschrieben.

Die 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: Die Objektdefinitionen für Benutzerkonten, auf welche die Suchkriterien angewendet werden können, sind vordefiniert. Sollten Sie weitere Objektdefinitionen benötigen, um beispielsweise die Vorauswahl der Benutzerkonten weiter einzuschränken, erzeugen Sie im Designer die entsprechenden kundenspezifische Objektdefinitionen. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um Kriterien für die Personenzuordnung festzulegen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > 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 10: Standardsuchkriterien für Benutzerkonten

Anwenden auf	Spalte an Person	Spalte am Benutzerkonto
SharePoint Online Benutzerkonten (benutzerauthentifiziert)	Standard-E-Mail-Adresse (`DefaultEmailAddress`)	E-Mail-Adresse (`EMail`)

5. Speichern Sie die Änderungen.

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

Verwandte Themen

- Automatische Zuordnung von Personen zu SharePoint Online Benutzerkonten auf Seite 73
- Personen suchen und direkt an Benutzerkonten zuordnen auf Seite 76

Automatisierungsgrade für SharePoint Online Benutzerkonten ändern

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

Um den Automatisierungsgrad für ein Benutzerkonto zu ändern

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Automatisierungsgrad** den Automatisierungsgrad.
5. Speichern Sie die Änderungen.

Personen suchen und direkt an Benutzerkonten zuordnen

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

Tabelle 11: Ansichten zur manuellen Zuordnung

Ansicht	Beschreibung
Vorgeschlagene Zuordnungen	Die Ansicht listet alle Benutzerkonten auf, denen der One Identity Manager eine Person zuordnen kann. Dazu werden die Personen angezeigt, die durch die Suchkriterien ermittelt und zugeordnet werden können.
Zugeordnete Benutzerkonten	Die Ansicht listet alle Benutzerkonten auf, denen eine Person zugeordnet ist.
Ohne Personenzuordnung	Die Ansicht listet alle Benutzerkonten auf, denen keine Person zugeordnet ist und für die über die Suchkriterien keine passende Person ermittelt werden kann.

Um Suchkriterien auf die Benutzerkonten anzuwenden

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Websitesammlungen**.
2. Wählen Sie in der Ergebnisliste die Websitesammlung.
3. Wählen Sie die Aufgabe **Suchkriterien für die Personenzuordnung definieren**.
4. Im unteren Bereich des Formulars klicken Sie **Neu laden**.

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

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

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

Um Personen direkt über die Vorschlagsliste zuzuordnen

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

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

  - ODER -

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

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

Um Zuordnungen zu entfernen

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

       Von den ausgewählten Benutzerkonten werden die zugeordneten Personen entfernt.

Kontendefinitionen an verbundene SharePoint Online Benutzerkonten zuweisen

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

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

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 Online > Benutzerkonten (benutzerauthentifiziert) > Verbunden aber nicht konfiguriert > <Websitesammlung>**.
    b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.
    c. Wählen Sie in der Auswahlliste **Kontendefinition** die Kontendefinition.
    d. Wählen Sie die Benutzerkonten, die die Kontendefinition erhalten sollen.
    e. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Kontendefinitionen an SharePoint Online Websitesammlungen zuweisen auf Seite 69

Personen manuell mit SharePoint Online Benutzerkonten verbinden

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

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

Um einer Person manuell Benutzerkonten zuzuweisen

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person und führen Sie die Aufgabe **SharePoint Online Benutzerkonten zuweisen** aus.
3. Weisen Sie die Benutzerkonten zu.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Anwendungsfälle für SharePoint Online Benutzerkonten auf Seite 79
- Unterstützte Typen von Benutzerkonten auf Seite 81

Anwendungsfälle für SharePoint Online Benutzerkonten

Beispiel:

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

Jan Bloggs soll ebenfalls einen Gastzugang für die Websitesammlung erhalten. Er besitzt ein Azure Active Directory Benutzerkonto in der selben Domäne. Im Web

Portal bestellt er die Mitgliedschaft in der Azure Active Directory Gruppe **Guests**. Sobald die Bestellung genehmigt und zugewiesen ist, kann er sich an der Websitesammlung anmelden.

Abhängig vom referenzierten Authentifizierungsobjekt werden SharePoint Online 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 Azure Active Directory 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 Online Rollen und Gruppen werden.
- Damit sich eine Person am SharePoint Online System anmelden kann, benötigt sie ein Azure Active Directory Benutzerkonto. Dieses Benutzerkonto muss Mitglied in der als Authentifizierungsobjekt genutzten Azure Active Directory Gruppe sein.
- Ein neues SharePoint Online 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 Azure Active Directory Benutzerkonto. Dieses Benutzerkonto kann im One Identity Manager als Authentifizierungsobjekt zugeordnet werden.
- Dem SharePoint Online Benutzerkonto kann eine Person zugeordnet werden. Damit kann das Benutzerkonto über Vererbung und über Direktzuweisung Mitglied in SharePoint Online 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 | SharePointOnline | PersonAutoFullsync** und **TargetSystem | SharePointOnline | PersonAutoDefault**.
- Ein neues SharePoint Online Benutzerkonto kann manuell oder über eine Kontendefinition erstellt werden. Das Azure Active Directory Benutzerkonto, das als Authentifizierungsobjekt genutzt wird, muss zu einer Domäne gehören dem das referenzierte Authentifizierungssystem vertraut.
- Das Benutzerkonto kann über eine Kontendefinition verwaltet werden.

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

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 12: Identitäten von Benutzerkonten

Identität	Beschreibung	Wert der Spalte IdentityType
Primäre Identität	Standardbenutzerkonto einer Person.	Primary
Organisatorische Identität	Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen.	Organizational
Persönliche Administratoridentität	Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird.	Admin
Zusatzidentität	Benutzerkonto, das für einen spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken.	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 Pseudo-Personen, die keinen Bezug zu einer realen Person haben. Diese Pseudo-Personen werden benötigt, um Berechtigungen an die Benutzerkonten vererben zu können. Bei der Auswertung von Berichten, Attestierungen oder Complianceprüfungen prüfen Sie, ob die Pseudo-Personen gesondert betrachtet werden müssen.

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

- Privilegiertes Benutzerkonto

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

Detaillierte Informationen zum Thema

- Standardbenutzerkonten auf Seite 82
- Administrative Benutzerkonten auf Seite 83
- Privilegierte Benutzerkonten auf Seite 86

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

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

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

Verwandte Themen

- Kontendefinitionen für SharePoint Online Benutzerkonten auf Seite 51

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**.

Verwandte Themen

- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 84
- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 85

Administrative Benutzerkonten für eine Person bereitstellen

Voraussetzungen

- Das Benutzerkonto muss als persönliche Administratoridentität gekennzeichnet sein.
- Die Person, die das Benutzerkonto nutzen soll, muss als persönliche Administratoridentität gekennzeichnet sein.
- Die Person, die das Benutzerkonto nutzen soll, muss mit einer Hauptidentität verbunden sein.

Um ein administratives Benutzerkonto für eine Person bereitzustellen

1. Kennzeichnen Sie das Benutzerkonto als persönliche Administratoridentität.
    a. Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (benutzerauthentifiziert)**.

       - ODER -

       Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (gruppenauthentifiziert).**
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Identität** den Wert **Persönliche Administratoridentität**.
2. Verbinden Sie das Benutzerkonto mit der Person, die dieses administrative Benutzerkonto nutzen soll.
    a. Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (benutzerauthentifiziert)**.

       - ODER -

       Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (gruppenauthentifiziert).**
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Person** die Person, die dieses administrative Benutzerkonto nutzt.

   TIPP: Als Zielsystemverantwortlicher können Sie über die Schaltfläche eine neue Person erstellen.

Verwandte Themen

- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 85
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Administrative Benutzerkonten für mehrere Personen bereitstellen

Voraussetzung

- Das Benutzerkonto muss als Gruppenidentität gekennzeichnet sein.
- Es muss eine Pseudo-Person vorhanden sein. Die Pseudo-Person muss als Gruppenidentität gekennzeichnet sein und muss einen Manager besitzen.
- Die Personen, die das Benutzerkonto nutzen dürfen, müssen als primäre Identitäten gekennzeichnet sein.

Um ein administratives Benutzerkonto für mehrere Personen bereitzustellen

1. Kennzeichnen Sie das Benutzerkonto als Gruppenidentität.
   a. Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (benutzerauthentifiziert)**.

      - ODER -

      Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (gruppenauthentifiziert).**
   b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
   c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
   d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Identität** den Wert **Gruppenidentität**.
2. Verbinden Sie das Benutzerkonto mit einer Pseudo-Person.
   a. Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (benutzerauthentifiziert)**.

      - ODER -

      Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (gruppenauthentifiziert).**

b. Wählen Sie in der Ergebnisliste das Benutzerkonto.

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

d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Person** die Pseudo-Person.

> TIPP: Als Zielsystemverantwortlicher können Sie über die Schaltfläche eine neue Pseudo-Person erstellen.

3. Weisen Sie dem Benutzerkonto die Personen zu, die dieses administrative Benutzerkonto nutzen sollen.

a. Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (benutzerauthentifiziert)**.

- ODER -

Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (gruppenauthentifiziert).**

b. Wählen Sie in der Ergebnisliste das Benutzerkonto.

c. Wählen Sie die Aufgabe **Personen mit Nutzungsberechtigungen zuzuweisen**.

d. 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 .

Verwandte Themen

- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 84
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

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 Abbildungsvorschriften für die Spalten `IsGroupAccount_Group` und `IsGroupAccount_RLAsgn` 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:

Verwandte Themen

- Kontendefinitionen für SharePoint Online Benutzerkonten auf Seite 51

Löschverzögerung für SharePoint Online Benutzerkonten festlegen

Über die Löschverzögerung legen Sie fest, wie lange die Benutzerkonten nach dem Auslösen des Löschens in der Datenbank verbleiben, bevor sie endgültig entfernt werden. Standardmäßig werden Benutzerkonten mit einer Löschverzögerung von 30 Tagen endgültig aus der Datenbank entfernt. Die Benutzerkonten werden zunächst deaktiviert oder 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.

Sie haben die folgenden Möglichkeiten die Löschverzögerung zu konfigurieren.

- Globale Löschverzögerung: Die Löschverzögerung gilt für die Benutzerkonten in allen Zielsystemen. Der Standardwert ist **30** Tage.

  Erfassen Sie eine abweichende Löschverzögerung im Designer für die Tabelle O3SUser in der Eigenschaft **Löschverzögerungen [Tage]**.

- Objektspezifische Löschverzögerung: Die Löschverzögerung kann abhängig von bestimmten Eigenschaften der Benutzerkonten konfiguriert werden.

  Um eine objektspezifische Löschverzögerung zu nutzen, erstellen Sie im Designer für die Tabelle O3SUser ein **Skript (Löschverzögerung)**.

  Beispiel:

  Die Löschverzögerung für privilegierte Benutzerkonten soll 10 Tage betragen. An der Tabelle wird folgendes **Skript (Löschverzögerung)** eingetragen.

  ```
  If $IsPrivilegedAccount:Bool$ Then
       Value = 10
  End If
  ```

Ausführliche Informationen zum Bearbeiten der Tabellendefinitionen und zum Konfigurieren der Löschverzögerung im Designer finden Sie im *One Identity Manager Konfigurationshandbuch*.

4

Managen von Zuweisungen von SharePoint Online Gruppen und Rollen

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

In einer SharePoint Online-Umgebung können die Benutzer verschiedene Berechtigungen haben, die folgendermaßen im One Identity Manager abgebildet werden:

- Berechtigung zur Nutzung von SharePoint Online Gruppen (Tabelle O3SGroup)
- Berechtigung zur Nutzung von SharePoint Online Rollen (Tabelle O3SRLAsgn)

Begriffe

- Eine SharePoint Online Rolle ist die mit einer konkreten Website verknüpfte Berechtigungsstufe.
- Die Zuweisung von Benutzerkonten oder Gruppen an eine SharePoint Online Rolle wird als Rollenzuweisung bezeichnet.
- Als Berechtigungszuweisungen werden die Zuweisungen der verschiedenen Berechtigungen an Benutzerkonten bezeichnet. Dazu gehören:
  - Zuweisungen von Gruppen an Benutzerkonten (Tabelle O3SUserInGroup)
  - Zuweisungen von Rollen an Benutzerkonten (Tabelle O3SUserHasRLAsgn)

Detaillierte Informationen zum Thema

- Zuweisen von SharePoint Online Berechtigungen an SharePoint Online Benutzerkonten auf Seite 90
- Wirksamkeit von SharePoint Online Berechtigungszuweisungen auf Seite 102

- Vererbung von SharePoint Online Gruppen anhand von Kategorien auf Seite 104
- Übersicht aller Zuweisungen auf Seite 107

Zuweisen von SharePoint Online Berechtigungen an SharePoint Online Benutzerkonten

Im One Identity Manager können SharePoint Online Berechtigungen direkt oder indirekt an Personen zugewiesen werden.

Bei der indirekten Zuweisung werden Personen und Berechtigungen in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der Berechtigungen, die einer Person zugewiesen ist. Wenn die Person ein SharePoint Online Benutzerkonto besitzt, dann erhält dieses Benutzerkonto die Berechtigungen.

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

Über Systemrollen können Berechtigungen zusammengefasst und als Paket an Personen zugewiesen werden. Sie können Systemrollen erstellen, die ausschließlich SharePoint Online Berechtigungen enthalten. Ebenso können Sie in einer Systemrolle beliebige Unternehmensressourcen zusammenfassen.

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

Ausführliche Informationen finden Sie in den folgenden Handbüchern.

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

Detaillierte Informationen zum Thema

- Voraussetzungen für indirekte Zuweisungen von SharePoint Online Berechtigungen an SharePoint Online Benutzerkonten auf Seite 91
- SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 93
- SharePoint Online Berechtigungen an Geschäftsrollen zuweisen auf Seite 94
- SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 99
- SharePoint Online Berechtigungen in Systemrollen aufnehmen auf Seite 95
- SharePoint Online Berechtigungen in den IT Shop aufnehmen auf Seite 96
- SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 100
- SharePoint Online Rollen an SharePoint Online Gruppen zuweisen auf Seite 100

Voraussetzungen für indirekte Zuweisungen von SharePoint Online Berechtigungen an SharePoint Online Benutzerkonten

Bei der indirekten Zuweisung werden Personen, SharePoint Online Gruppen und SharePoint Online Rollen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Für die indirekte Zuweisung von SharePoint Online Gruppen und SharePoint Online Rollen prüfen Sie folgende Einstellungen und passen Sie die Einstellungen bei Bedarf an.

Voraussetzungen für die indirekte Zuweisung von SharePoint Online Gruppen an die SharePoint Online Benutzerkonten von Personen

1. Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und SharePoint Online Gruppen erlaubt.
2. Am SharePoint Online Benutzerkonto ist die Option **Gruppenauthentifiziert** deaktiviert.
3. Das SharePoint Online Benutzerkonto sind mit der Option **Gruppen erbbar** gekennzeichnet.
4. Das SharePoint Online Benutzerkonto ist mit einer Person verbunden.
5. Das SharePoint Online Benutzerkonto und die SharePoint Online Gruppen gehören zur selben Websitesammlung.

Voraussetzungen für die indirekte Zuweisung von SharePoint Online Rollen an die SharePoint Online Benutzerkonten von Personen

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und SharePoint Online Rollen erlaubt.
- Am SharePoint Online Benutzerkonto ist die Option **Gruppenauthentifiziert** deaktiviert.
- Das SharePoint Online Benutzerkonto sind mit der Option **Rollen erbbar** gekennzeichnet.
- Das SharePoint Online Benutzerkonto ist mit einer Person verbunden.
- Das SharePoint Online Benutzerkonto und die SharePoint Online Rollen gehören zur selben Websitesammlung.

Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

1. Wählen Sie im Manager in der Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.

   - ODER -

   Wählen Sie im Manager in der Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.
2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
   - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
   - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
3. Speichern Sie die Änderungen.

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

HINWEIS: Bei der Vererbung von Unternehmensressourcen über Abteilungen, Kostenstellen, Standorte und Geschäftsrollen spielen unter Umständen weitere Konfigurationseinstellungen eine Rolle. So kann beispielsweise die Vererbung für eine Rolle blockiert sein oder die Vererbung an Personen nicht erlaubt sein. Ausführliche Informationen über die Grundlagen zur Zuweisung von Unternehmensressourcen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- Stammdaten für SharePoint Online Benutzerkonten bearbeiten auf Seite 115
- Stammdaten für benutzerauthentifizierte Benutzerkonten auf Seite 115

SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie Gruppen und Rollen an Abteilungen, Kostenstellen oder Standorte zu, damit sie über diese Organisationen an Benutzerkonten zugewiesen werden.

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

1. Wählen Sie im Manager eine der folgenden Kategorien.
   - **SharePoint Online > Gruppen**
   - **SharePoint Online > Rollen**
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

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

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

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

1. Wählen Sie 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 eine der folgenden Aufgaben.
   - **SharePoint Online Gruppen zuweisen**
   - **SharePoint Online Rollen zuweisen**
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungen zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Berechtigung und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von SharePoint Online Berechtigungen an SharePoint Online Benutzerkonten auf Seite 91
- SharePoint Online Berechtigungen an Geschäftsrollen zuweisen auf Seite 94
- SharePoint Online Berechtigungen in Systemrollen aufnehmen auf Seite 95
- SharePoint Online Berechtigungen in den IT Shop aufnehmen auf Seite 96
- SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 99
- SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 100
- One Identity Manager Benutzer für die Verwaltung einer SharePoint Online-Umgebung auf Seite 9

SharePoint Online Berechtigungen an Geschäftsrollen zuweisen

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

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

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

1. Wählen Sie im Manager eine der folgenden Kategorien.
   - **SharePoint Online > Gruppen**
   - **SharePoint Online > Rollen**
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Um Berechtigungen an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen > <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie eine der folgenden Aufgaben.
   - **SharePoint Online Gruppen zuweisen**
   - **SharePoint Online Rollen zuweisen**
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von SharePoint Online Berechtigungen an SharePoint Online Benutzerkonten auf Seite 91
- SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 93
- SharePoint Online Berechtigungen in Systemrollen aufnehmen auf Seite 95
- SharePoint Online Berechtigungen in den IT Shop aufnehmen auf Seite 96
- SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 99
- SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 100
- One Identity Manager Benutzer für die Verwaltung einer SharePoint Online-Umgebung auf Seite 9

SharePoint Online Berechtigungen in Systemrollen aufnehmen

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

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

HINWEIS: 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 Berechtigung an Systemrollen zuzuweisen

1. Wählen Sie im Manager eine der folgenden Kategorien.
   - **SharePoint Online > Gruppen**
   - **SharePoint Online > Rollen**
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

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

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

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von SharePoint Online Berechtigungen an SharePoint Online Benutzerkonten auf Seite 91
- SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 93
- SharePoint Online Berechtigungen an Geschäftsrollen zuweisen auf Seite 94
- SharePoint Online Berechtigungen in den IT Shop aufnehmen auf Seite 96
- SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 99
- SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 100

SharePoint Online Berechtigungen in den IT Shop aufnehmen

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

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

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

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

Um eine Berechtigung in den IT Shop aufzunehmen

1. Wählen Sie im Manager eine der folgenden Kategorien (bei nicht-rollenbasierter Anmeldung).
   - **SharePoint Online > Gruppen**
   - **SharePoint Online > Rollen**

   - ODER -

   Wählen Sie im Manager eine der folgenden Kategorien (bei rollenbasierter Anmeldung).
   - **Berechtigungen > SharePoint Online Gruppen**
   - **Berechtigungen > SharePoint Online Rollen**
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Wählen Sie den Tabreiter **IT Shop Strukturen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigung an die IT Shop Regale zu.
6. Speichern Sie die Änderungen.

Um eine Berechtigung aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager eine der folgenden Kategorien (bei nicht-rollenbasierter Anmeldung).
   - **SharePoint Online > Gruppen**
   - **SharePoint Online > Rollen**

   - ODER -

   Wählen Sie im Manager eine der folgenden Kategorien (bei rollenbasierter Anmeldung).

- **Berechtigungen > SharePoint Online Gruppen**
- **Berechtigungen > SharePoint Online Rollen**

2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Wählen Sie den Tabreiter **IT Shop Strukturen**.
5. Entfernen Sie im Bereich **Zuordnungen entfernen** die Berechtigung aus den IT Shop Regalen.
6. Speichern Sie die Änderungen.

Um eine Berechtigung aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager eine der folgenden Kategorien (bei nicht-rollenbasierter Anmeldung).
   - **SharePoint Online > Gruppen**
   - **SharePoint Online > Rollen**

   - ODER -

   Wählen Sie im Manager eine der folgenden Kategorien (bei rollenbasierter Anmeldung).
   - **Berechtigungen > SharePoint Online Gruppen**
   - **Berechtigungen > SharePoint Online Rollen**
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

- Stammdaten für SharePoint Online Gruppen auf Seite 126
- Allgemeine Stammdaten für SharePoint Online Rollen auf Seite 142
- Voraussetzungen für indirekte Zuweisungen von SharePoint Online Berechtigungen an SharePoint Online Benutzerkonten auf Seite 91
- SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 93
- SharePoint Online Berechtigungen an Geschäftsrollen zuweisen auf Seite 94
- SharePoint Online Berechtigungen in Systemrollen aufnehmen auf Seite 95

- SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 99
- SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 100
- One Identity Manager Benutzer für die Verwaltung einer SharePoint Online-Umgebung auf Seite 9

SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen

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

Um eine Berechtigung direkt an Benutzerkonten zuzuweisen

1. Wählen Sie im Manager eine der folgenden Kategorien.
   - **SharePoint Online > Gruppen**
   - **SharePoint Online > Rollen**
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 100
- SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 93
- SharePoint Online Berechtigungen an Geschäftsrollen zuweisen auf Seite 94
- SharePoint Online Berechtigungen in Systemrollen aufnehmen auf Seite 95
- SharePoint Online Berechtigungen in den IT Shop aufnehmen auf Seite 96

SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Berechtigungen direkt zuweisen. Berechtigungen, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Um Berechtigungen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie eine der folgenden Aufgaben.
   - **Gruppen zuweisen**
   - **SharePoint Online Rollen zuweisen**
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungen zu.

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

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

Verwandte Themen

- SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 99
- SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 93
- SharePoint Online Berechtigungen an Geschäftsrollen zuweisen auf Seite 94
- SharePoint Online Berechtigungen in Systemrollen aufnehmen auf Seite 95
- SharePoint Online Berechtigungen in den IT Shop aufnehmen auf Seite 96

SharePoint Online Rollen an SharePoint Online Gruppen zuweisen

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

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

Um SharePoint Online Rollen an eine Gruppe zuzuweisen

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

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Stammdaten für SharePoint Online Berechtigungsstufen auf Seite 131
- SharePoint Online Gruppen an SharePoint Online Rollen zuweisen auf Seite 101
- SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 93
- SharePoint Online Berechtigungen an Geschäftsrollen zuweisen auf Seite 94
- SharePoint Online Berechtigungen in Systemrollen aufnehmen auf Seite 95
- SharePoint Online Berechtigungen in den IT Shop aufnehmen auf Seite 96
- SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 99
- SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 100

SharePoint Online Gruppen an SharePoint Online Rollen zuweisen

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

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

Um Gruppen an eine SharePoint Online Rolle zuzuweisen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > 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.

   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

- Stammdaten für SharePoint Online Berechtigungsstufen auf Seite 131
- SharePoint Online Rollen an SharePoint Online Gruppen zuweisen auf Seite 100
- SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 93
- SharePoint Online Berechtigungen an Geschäftsrollen zuweisen auf Seite 94
- SharePoint Online Berechtigungen in Systemrollen aufnehmen auf Seite 95
- SharePoint Online Berechtigungen in den IT Shop aufnehmen auf Seite 96
- SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 99
- SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 100

Wirksamkeit von SharePoint Online Berechtigungszuweisungen

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 `O3SUserInO3SGroup` und `O3SBaseTreeHasGroup` über die Spalte `XIsInEffect` abgebildet.

Beispiel: Wirksamkeit von Gruppenmitgliedschaften

- 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 13: Festlegen der ausgeschlossenen Gruppen (Tabelle `O3SGroupExclusion`)

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

Tabelle 14: 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 15: 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.

  Aktivieren Sie im Designer den Konfigurationsparameter und kompilieren Sie die Datenbank.

  HINWEIS: Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Sich ausschließende Gruppen gehören zur selben Websitesammlung.

Um Gruppen auszuschließen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > 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 Online 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 63**.

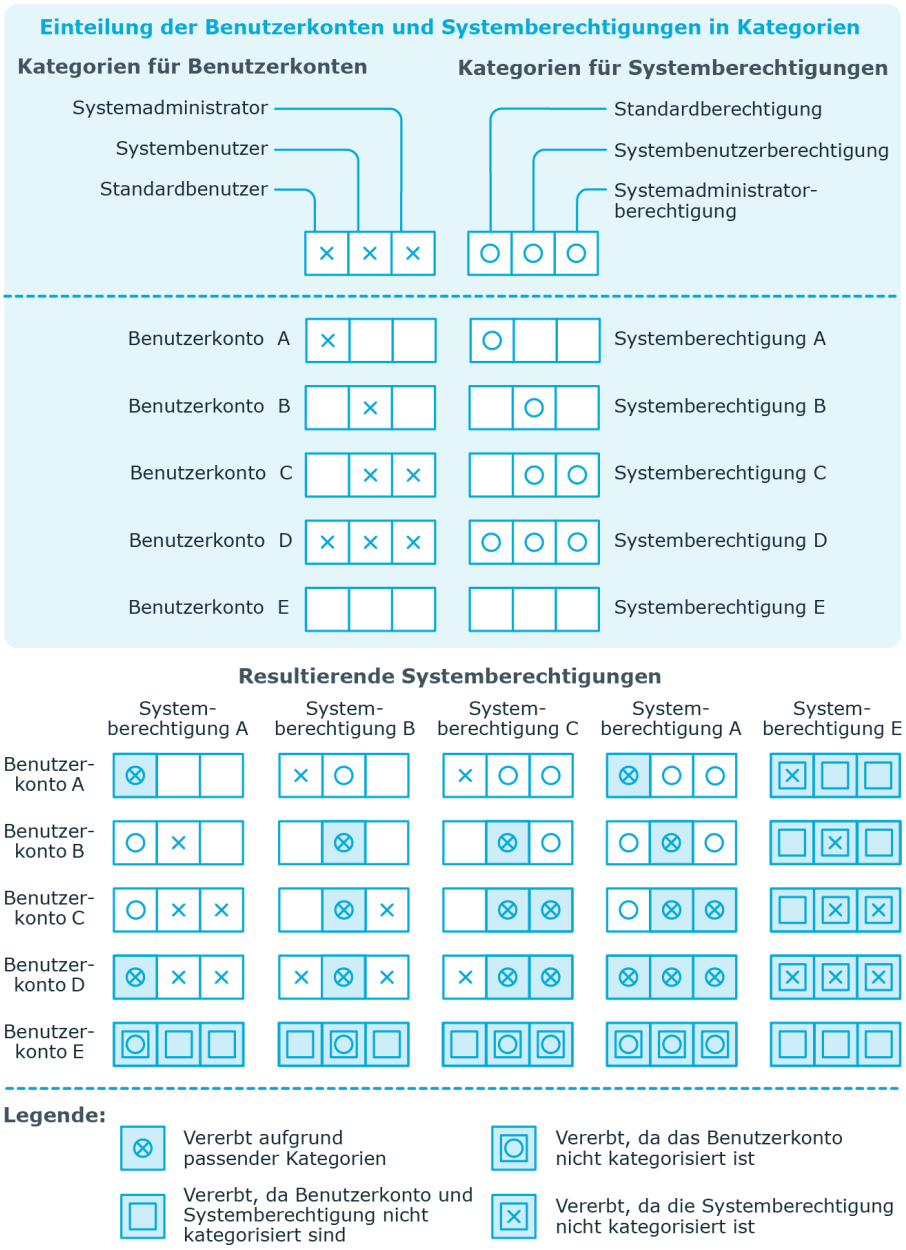
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto vererbt. Ist 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 16: Beispiele für Kategorien

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

Abbildung 2: Beispiel für die Vererbung über Kategorien



Um die Vererbung über Kategorien zu nutzen

1. Definieren Sie im Manager an der Websitesammlung die Kategorien.
2. Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
3. Weisen Sie die Kategorien den Gruppen über ihre Stammdaten zu.

Verwandte Themen

- Kategorien für die Vererbung von SharePoint Online Gruppen definieren auf Seite 135
- Stammdaten für gruppenauthentifizierte Benutzerkonten auf Seite 120
- Stammdaten für benutzerauthentifizierte Benutzerkonten auf Seite 115
- Stammdaten für SharePoint Online Gruppen auf Seite 126

Übersicht aller Zuweisungen

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

Beispiele:

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

Um detaillierte Informationen über Zuweisungen anzuzeigen

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

  Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Personen befinden, denen das ausgewählte Basisobjekt zugewiesen ist. Die Bedeutung der Steuerelemente des

Berichts ist in einer separaten Legende erläutert. Die Legende erreichen Sie über das Symbol in der Symbolleiste des Berichtes.

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

Abbildung 3: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 17: Bedeutung der Symbole in der Symbolleiste des Berichts

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

Abbilden von SharePoint Online Objekten im One Identity Manager

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

Detaillierte Informationen zum Thema

SharePoint Online Mandanten

Ein SharePoint Online Mandant ist das Basisobjekt einer SharePoint Online-Umgebung. Ein SharePoint Online Mandant hat zwingend eine direkte Beziehung zu einem Azure Active Directory Mandanten. Es gibt für jede verbundene SharePoint Online-Umgebung nur einen Mandanten.

SharePoint Online Mandanten werden benötigt, um Provisionierungsprozesse, die automatische Zuordnung von Personen zu Benutzerkonten und die Vererbung von Gruppen an Benutzerkonten über Kategorien innerhalb einer SharePoint Online zu konfigurieren.

HINWEIS: SharePoint Online Mandanten können im One Identity Manager nicht erstellt werden. Die Einrichtung der SharePoint Online Mandanten in der One Identity Manager-Datenbank übernimmt der Synchronization Editor.

Detaillierte Informationen zum Thema

- Stammdaten von SharePoint Online Mandanten anzeigen und bearbeiten auf Seite 110
- Allgemeine Stammdaten für SharePoint Online Mandanten auf Seite 110
- Synchronisieren einer SharePoint Online-Umgebung auf Seite 13
- Verarbeitung von Systemobjekten auf Seite 166

Stammdaten von SharePoint Online Mandanten anzeigen und bearbeiten

Sie können im einzelne Stammdaten des Mandanten bearbeiten. Neue Mandanten können Sie nicht erstellen.

Um die Stammdaten eines SharePoint Online Mandanten zu bearbeiten

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Mandanten**.
2. Wählen Sie in der Ergebnisliste den Mandanten.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für einen Mandanten.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für SharePoint Online Mandanten auf Seite 110

Allgemeine Stammdaten für SharePoint Online Mandanten

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

Tabelle 18: Allgemeine Stammdaten eines SharePoint Online Mandanten

Eigenschaft	Beschreibung
Bezeichnung	Name der Organisation, die für die Anmeldung an Office 365 benutzt wird.
Azure Active Directory Mandant	Eindeutige Bezeichnung des Azure Active Directory Mandanten.

Eigenschaft	Beschreibung
Zielsystemverantwortliche	Anwendungsrolle, in der die Zielsystemverantwortlichen des Mandanten festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte des Mandanten, dem sie zugeordnet sind. Jedem Mandanten können andere Zielsystemverantwortliche zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle aus, deren Mitglieder verantwortlich für die Administration dieses Mandanten sind. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.
Synchronisiert durch	Art der Synchronisation, über welche die Daten zwischen dem Mandanten und dem One Identity Manager ausgetauscht werden. Sobald Objekte für diesen Mandanten im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden. Beim Erstellen eines Mandanten mit dem Synchronization Editor wird **One Identity Manager** verwendet. **Tabelle 19: Zulässige Werte** **Wert** / **Synchronisation durch** / **Provisionierung durch** One Identity Manager / SharePoint Online Konnektor / SharePoint Online Konnektor Keine Synchronisation / keine / keine HINWEIS: Wenn Sie **Keine Synchronisation** festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.
Stammwebsite-URL	Basis-Websitesammlung für den Mandanten.
Kompatibilitätsbereich	Gibt an, welcher Kompatibilitätsbereich für neue Websitesammlungen verfügbar ist.
Kontingent Ressource	Gibt den Wert des Kontingents Ressource für den Mandanten an.
Kontingent Ressource Verbrauch	Gibt den Wert des Kontingents Ressourcen an, den alle Websites des Mandanten nutzen.
Forderungsgruppe "Alle Benutzer" anzeigen	Ermöglicht es dem Administrator, die Forderungsgruppe **Alle Benutzer** in der Personenauswahl auszublenden.

Eigenschaft	Beschreibung
Forderungsgruppe "Jeder" anzeigen	Ermöglicht es dem Administrator, die Forderungsgruppe **Jeder** in der Personenauswahl auszublenden.
Forderungsgruppe "Jeder, außer externen Benutzern" anzeigen	Ermöglicht es dem Administrator, die Forderungsgruppe **Jeder, außer externen Benutzern** in der Personenauswahl auszublenden.

Verwandte Themen

- Zielsystemverantwortliche auf Seite 159

Zusätzliche Aufgaben zur Verwaltung von SharePoint Online Mandanten

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

Aufgabe	Thema
Überblick über den SharePoint Online Mandanten	Überblick über SharePoint Online Mandanten auf Seite 112
Suchkriterien für die Personenzuordnung definieren	Suchkriterien für die automatische Personenzuordnung bearbeiten auf Seite 74
Synchronisationsprojekt bearbeiten	Synchronisationsprojekt für einen SharePoint Online Mandanten bearbeiten auf Seite 113
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 43

Überblick über SharePoint Online Mandanten

Um einen Überblick über einen Mandanten zu erhalten

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Mandanten**.
2. Wählen Sie in der Ergebnisliste den Mandanten.
3. Wählen Sie die Aufgabe **Überblick über den SharePoint Online Mandanten**.

Synchronisationsprojekt für einen SharePoint Online Mandanten bearbeiten

Synchronisationsprojekte, in denen ein Azure Active Directory Mandant bereits als Basisobjekt verwendet wird, können auch über den Manager geöffnet werden. In diesem Modus können beispielsweise die Konfigurationseinstellungen überprüft oder die Synchronisationsprotokolle eingesehen werden. Der Synchronization Editor wird nicht mit seinem vollen Funktionsumfang gestartet. Verschiedene Funktionen, wie Simulieren oder Ausführen einer Synchronisation, Starten des Zielsystembrowsers und andere, können nicht ausgeführt werden.

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

Um ein bestehendes Synchronisationsprojekt im Synchronization Editor zu öffnen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Mandanten**.
2. Wählen Sie in der Ergebnisliste den Mandanten.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten**.

Verwandte Themen

- Anpassen einer Synchronisationskonfiguration auf Seite 31

SharePoint Online Benutzerkonten

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

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

- Azure Active Directory Gruppen vom Typ **Sicherheitsgruppe** (Tabelle AADGroup)
- Azure Active Directory Benutzerkonten (Tabelle AADUser)

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

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

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

HINWEIS:

Verwandte Themen

- Anwendungsfälle für SharePoint Online Benutzerkonten auf Seite 79
- Managen von SharePoint Online Benutzerkonten und Personen auf Seite 50
- Kontendefinitionen für SharePoint Online Benutzerkonten auf Seite 51
- SharePoint Online Benutzerkonten erstellen auf Seite 114
- Stammdaten für SharePoint Online Benutzerkonten bearbeiten auf Seite 115
- SharePoint Online Benutzerkonten löschen und wiederherstellen auf Seite 124
- Managen von Zuweisungen von SharePoint Online Gruppen und Rollen auf Seite 89

SharePoint Online Benutzerkonten erstellen

Um ein Benutzerkonto zu erstellen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (benutzerauthentifiziert)**.

   - ODER -

   Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (gruppenauthentifiziert).**
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für benutzerauthentifizierte Benutzerkonten auf Seite 115
- Stammdaten für gruppenauthentifizierte Benutzerkonten auf Seite 120

- Stammdaten für SharePoint Online Benutzerkonten bearbeiten auf Seite 115

Stammdaten für SharePoint Online Benutzerkonten bearbeiten

Um die Stammdaten eines Benutzerkontos zu bearbeiten

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (benutzerauthentifiziert)**.

   - ODER -

   Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (gruppenauthentifiziert).**
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Benutzerkontos.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für benutzerauthentifizierte Benutzerkonten auf Seite 115
- Stammdaten für gruppenauthentifizierte Benutzerkonten auf Seite 120
- SharePoint Online Benutzerkonten erstellen auf Seite 114
- SharePoint Online Benutzerkonten löschen und wiederherstellen auf Seite 124

Stammdaten für benutzerauthentifizierte Benutzerkonten

Für ein benutzerauthentifiziertes Benutzerkonto erfassen Sie die folgenden Stammdaten.

Tabelle 20: 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

Eigenschaft	Beschreibung
	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.
Keine Verbindung mit einer Person erforderlich	Gibt an, ob dem Benutzerkonto absichtlich keine Person zugeordnet ist. Die Option wird automatisch aktiviert, wenn ein Benutzerkonto in der Ausschlussliste für die automatische Personenzuordnung enthalten ist oder eine entsprechende Attestierung erfolgt ist. Sie können die Option manuell setzen. Aktivieren Sie die Option, falls das Benutzerkonto mit keiner Person verbunden werden muss (beispielsweise, wenn mehrere Personen das Benutzerkonto verwenden). Wenn durch die Attestierung diese Benutzerkonten genehmigt werden, werden diese Benutzerkonten künftig nicht mehr zur Attestierung vorgelegt. Im Web Portal können Benutzerkonten, die nicht mit einer Person verbunden sind, nach verschiedenen Kriterien gefiltert werden.
Nicht mit einer Person verbunden	Zeigt an, warum für das Benutzerkonto die Option **Keine Verbindung mit einer Person erforderlich** aktiviert ist. Mögliche Werte sind: • **durch Administrator**: Die Option wurde manuell durch den Administrator aktiviert. • **durch Attestierung**: Das Benutzerkonto wurde attestiert. • **durch Ausschlusskriterium**: Das Benutzerkonto wird aufgrund eines Ausschlusskriteriums nicht mit einer Person verbunden. Das Benutzerkonto ist beispielsweise in der Ausschlussliste für die automatische Personenzuordnung enthalten (Konfigurationsparameter **PersonExcludeList**).
Kontendefinition	Kontendefinition, über die das Benutzerkonto erstellt wurde. Die Kontendefinition wird benutzt, um die Stammdaten des Benutzerkontos automatisch zu befüllen und um einen Automatisierungsgrad für das Benutzerkonto festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der

Eigenschaft	Beschreibung
	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: Über die Aufgabe **Entferne Kontendefinition** am Benutzerkonto können Sie das Benutzerkonto wieder in den Zustand **Linked** zurücksetzen. Dabei wird die Kontendefinition vom Benutzerkonto und von der Person entfernt. Das Benutzerkonto bleibt über diese Aufgabe erhalten, wird aber nicht mehr über die Kontendefinition verwaltet. Die Aufgabe entfernt nur Kontendefinitionen, die direkt zugewiesen sind (`XOrigin=1`). HINWEIS: Sollen Personen ihre SharePoint Online Benutzerkonten über Kontendefinitionen erhalten, müssen die Personen Benutzerkonten im Azure Active Directory Mandanten besitzen, der am SharePoint Online Mandanten hinterlegt ist.
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.
Websitesammlung	Websitesammlung, in der das Benutzerkonto genutzt wird.
Prinzipal-Typ	Art des Prinzipals (Benutzer, Domänengruppe).
Authentifizierungsmodus	Authentifizierungsmodus, der bei der Anmeldung mit diesem Benutzerkonto am SharePoint Online genutzt wird. Für SharePoint Online gilt **AzureAD** als einziger Authentifizierungsmodus.
Authentifizierungsobjekt	Authentifizierungsobjekt, welches das Benutzerkonto referenziert. 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: • Azure Active Directory Benutzerkonten aus dem Mandaten, der dem SharePoint Online Mandanten

Eigenschaft	Beschreibung
	zugeordnet ist HINWEIS: Das SharePoint Online Benutzerkonto wird auch dann erstellt, wenn das Benutzerkonto, das als Authentifizierungsobjekt genutzt wird, deaktiviert oder gesperrt ist.
Titel	Beliebiger Anzeigename des Benutzerkontos. Der Titel wird standardmäßig aus dem Anzeigenamen des Authentifizierungsobjektes gebildet. Wenn kein Authentifizierungsobjekt zugeordnet ist, tragen Sie den Anzeigenamen manuell ein.
Anmeldename	Anmeldename des Benutzerkontos. Der Anmeldename wird über eine Bildungsregel ermittelt. Wenn kein Authentifizierungsobjekt zugeordnet ist, tragen Sie den Anmeldenamen manuell ein.
E-Mail-Adresse	E-Mail-Adresse des Benutzerkontos. Die E-Mail-Adresse wird über Bildungsregeln aus der E-Mail-Adresse des Authentifizierungsobjektes gebildet.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten SharePoint Online 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 Auswahlliste eine oder mehrere Kategorien.
Identität	Typ der Identität des Benutzerkontos. Zulässige Werte sind: • **Primäre Identität**: Standardbenutzerkonto einer Person. • **Organisatorische Identität**: Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen. • **Persönliche Administratoridentität**: Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird. • **Zusatzidentität**: Benutzerkonto, das für einen spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken.

Eigenschaft	Beschreibung
	• **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	Gibt an, ob das Benutzerkonto Gruppen über die verbundene Person erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Person Mitglied ist, oder über 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.
Rollen erbbar	Gibt an, ob das Benutzerkonto SharePoint Online Rollen über die verbundene Person erben darf. Ist die Option aktiviert, werden SharePoint Online Rollen über hierarchische Rollen, in denen die Person Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt.
Administrator	Angabe, ob das Benutzerkonto Administrator einer Websitesammlung ist.
Versteckt	Angabe, ob das Benutzerkonto in der Benutzeroberfläche angezeigt wird.

Verwandte Themen

- Kontendefinitionen für SharePoint Online Benutzerkonten auf Seite 51
- Kategorien für die Vererbung von SharePoint Online Gruppen definieren auf Seite 135
- Voraussetzungen für indirekte Zuweisungen von SharePoint Online Berechtigungen an SharePoint Online Benutzerkonten auf Seite 91
- Automatische Zuordnung von Personen zu SharePoint Online Benutzerkonten auf Seite 73
- Unterstützte Typen von Benutzerkonten auf Seite 81

Stammdaten für gruppenauthentifizierte Benutzerkonten

Für ein gruppenauthentifiziertes Benutzerkonto erfassen Sie die folgenden Stammdaten.

Tabelle 21: Stammdaten eines gruppenauthentifizierten 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.
Keine Verbindung mit einer Person erforderlich	Gibt an, ob dem Benutzerkonto absichtlich keine Person zugeordnet ist.Sie können die Option manuell setzen. Aktivieren Sie die Option, falls das Benutzerkonto mit keiner Person verbunden werden muss (beispielsweise, wenn mehrere Personen das Benutzerkonto verwenden). Wenn durch die Attestierung diese Benutzerkonten genehmigt werden, werden diese Benutzerkonten künftig nicht mehr zur Attestierung vorgelegt. Im Web Portal können Benutzerkonten, die nicht mit einer Person verbunden sind, nach verschiedenen Kriterien gefiltert werden.
Nicht mit einer Person verbunden	Zeigt an, warum für das Benutzerkonto die Option **Keine Verbindung mit einer Person erforderlich** aktiviert ist. Das Benutzerkonto wird aufgrund eines Ausschlusskriteriums nicht mit einer Person verbunden.
Websitesammlung	Websitesammlung, in der das Benutzerkonto genutzt wird.
Gruppenauthentifiziert	Angabe, ob das Authentifizierungsobjekt des Benutzerkontos eine Gruppe ist.

Eigenschaft	Beschreibung
Authentifizierungsmodus	Authentifizierungsmodus, der bei der Anmeldung mit diesem Benutzerkonto am SharePoint Online Server genutzt wird. Für SharePoint Online gilt **AzureAD** als einziger Authentifizierungsmodus.
Authentifizierungsobjekt	Authentifizierungsobjekt, welches das Benutzerkonto referenziert. 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: • Azure Active Directory Gruppen mit dem Gruppentyp **Sicherheitsgruppe** aus dem Mandaten, der dem SharePoint Online Mandanten zugeordnet ist
Titel	Beliebiger Anzeigename des Benutzerkontos. Der Titel standardmäßig aus dem Anzeigenamen des Authentifizierungsobjektes gebildet. Wenn kein Authentifizierungsobjekt zugeordnet ist, tragen Sie den Anzeigenamen manuell ein.
Anmeldename	Anmeldename des Benutzerkontos. Der Anmeldename wird über eine Bildungsregel ermittelt. Wenn kein Authentifizierungsobjekt zugeordnet ist, tragen Sie den Anmeldenamen manuell ein.
E-Mail-Adresse	E-Mail-Adresse des Benutzerkontos. Die E-Mail-Adresse wird über Bildungsregeln aus der E-Mail-Adresse des Authentifizierungsobjektes gebildet.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten SharePoint Online 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 Auswahlliste eine oder mehrere Kategorien.
Hinweise	Freitextfeld für zusätzliche Erläuterungen.

Eigenschaft	Beschreibung
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 für einen spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken. • **Gruppenidentität**: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird. Weisen Sie alle Personen zu, die das Benutzerkonto nutzen. • **Dienstidentität**: Dienstkonto.
Privilegiertes Benutzerkonto	Gibt an, ob es sich um ein privilegiertes Benutzerkonto handelt.
Administrator	Gibt an, ob das Benutzerkonto Administrator einer Websitesammlung ist.
Versteckt	Gibt an, ob das Benutzerkonto in der Benutzeroberfläche angezeigt wird.

Verwandte Themen

- Kategorien für die Vererbung von SharePoint Online Gruppen definieren auf Seite 135
- Unterstützte Typen von Benutzerkonten auf Seite 81

Zusätzliche Aufgaben zur Verwaltung von SharePoint Online Benutzerkonten

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

Aufgabe	Thema
Überblick über das SharePoint Online Benutzerkonto	Überblick über SharePoint Online Benutzerkonten auf Seite 123
Zusatzeigenschaften zuweisen	Zusatzeigenschaften an SharePoint Online Benutzerkonten zuweisen auf Seite 123
Gruppen zuweisen	SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 100
SharePoint Online Rollen zuweisen	SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 100
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 43

Überblick über SharePoint Online Benutzerkonten

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (benutzerauthentifiziert)**.

   - ODER -

   Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (gruppenauthentifiziert).**
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das SharePoint Online Benutzerkonto**.

Zusatzeigenschaften an SharePoint Online Benutzerkonten zuweisen

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

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

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (benutzerauthentifiziert)**.

   - ODER -

   Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (gruppenauthentifiziert).**

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.

   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.

SharePoint Online Benutzerkonten löschen und wiederherstellen

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.

Ein Benutzerkonto, das nicht über eine Kontendefinition entstanden ist, löschen Sie über die Ergebnisliste oder über die Menüleiste. Nach Bestätigung der Sicherheitsabfrage wird das Benutzerkonto im One Identity Manager zunächst zum Löschen markiert. Das Benutzerkonto wird im One Identity Manager gesperrt und je nach Einstellung der Löschverzögerung endgültig aus der One Identity Manager-Datenbank und aus dem Zielsystem gelöscht.

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

Um ein Benutzerkonto zu löschen, das nicht über eine Kontendefinition verwaltet wird

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (benutzerauthentifiziert)**.

   - ODER -

   Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (gruppenauthentifiziert).**
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Um ein Benutzerkonto wiederherzustellen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (benutzerauthentifiziert)**.

   - ODER -

   Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (gruppenauthentifiziert).**
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste  .

Verwandte Themen

- Löschverzögerung für SharePoint Online Benutzerkonten festlegen auf Seite 88

SharePoint Online Gruppen

Gruppen werden in SharePoint Online 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 Online Rollen werden direkt an Gruppen zugewiesen. Alle Benutzerkonten, die Mitglied dieser Gruppen sind, erhalten die in den SharePoint Online Rollen definierten Berechtigungen auf diese Website. Um Benutzer in Gruppen aufzunehmen, können Sie die Gruppen direkt an die Benutzer zuweisen. Sie können Gruppen an Abteilungen, Kostenstellen, Standorte, Geschäftsrollen, Systemrollen oder den IT Shop zuweisen.

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

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

Verwandte Themen

- SharePoint Online Gruppen erstellen auf Seite 126
- Stammdaten für SharePoint Online Gruppen bearbeiten auf Seite 126
- Stammdaten für SharePoint Online Gruppen auf Seite 126
- SharePoint Online Gruppen löschen auf Seite 130
- Managen von Zuweisungen von SharePoint Online Gruppen und Rollen auf Seite 89

SharePoint Online Gruppen erstellen

Um eine Gruppe zu erstellen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Gruppen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für SharePoint Online Gruppen auf Seite 126
- Stammdaten für SharePoint Online Gruppen bearbeiten auf Seite 126
- SharePoint Online Gruppen löschen auf Seite 130

Stammdaten für SharePoint Online Gruppen bearbeiten

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für SharePoint Online Gruppen auf Seite 126
- SharePoint Online Gruppen erstellen auf Seite 126
- SharePoint Online Gruppen löschen auf Seite 130

Stammdaten für SharePoint Online Gruppen

Für eine Gruppe erfassen Sie die folgenden Stammdaten.

Tabelle 22: Stammdaten einer SharePoint Online Gruppe

Eigenschaft	Beschreibung
Titel	Anzeigename der Gruppe.
Websitesammlung	Websitesammlung, in der die Gruppe angewendet wird.
Eigentümer	Eigentümer der Gruppe. Es kann entweder ein SharePoint Online Benutzerkonto oder eine SharePoint Online Gruppe ausgewählt werden.
Leistungsposition	Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Benutzerkonten. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen zur Risikobewertung finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
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.
Versteckt	Angabe, ob die Gruppe in der Benutzeroberfläche angezeigt wird.
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 Online Benutzer die Mitgliedschaft in dieser Gruppe selbst beantragen oder beenden dürfen.
Auf Antrag automatische Mitgliedschaft	Angabe, ob SharePoint Online 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	Gibt an, ob die Gruppe über den IT Shop bestellbar ist. Ist die

Eigenschaft	Beschreibung
	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	Gibt an, 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

- Vererbung von SharePoint Online Gruppen anhand von Kategorien auf Seite 104
- SharePoint Online Berechtigungen in den IT Shop aufnehmen auf Seite 96

Zusätzliche Aufgaben zur Verwaltung von SharePoint Online Gruppen

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

Aufgabe	Thema
Überblick über die SharePoint Online Gruppe	Überblick über SharePoint Online Gruppen auf Seite 129
Benutzerkonten zuweisen	SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 99
SharePoint Online Rollen zuweisen	SharePoint Online Rollen an SharePoint Online Gruppen zuweisen auf Seite 100
Systemrollen zuweisen	SharePoint Online Berechtigungen in Systemrollen aufnehmen auf Seite 95
Geschäftsrollen zuweisen	SharePoint Online Berechtigungen an Geschäftsrollen zuweisen auf Seite 94
Organisationen zuweisen	SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 93
Gruppen ausschließen	Wirksamkeit von SharePoint Online Berechtigungszuweisungen auf Seite 102

Aufgabe	Thema
In IT Shop aufnehmen	SharePoint Online Berechtigungen in den IT Shop aufnehmen auf Seite 96
Zusatzeigenschaften zuweisen	Zusatzeigenschaften an SharePoint Online Gruppen zuweisen auf Seite 129
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 43

Überblick über SharePoint Online Gruppen

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 im Manager die Kategorie **SharePoint Online > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Online Gruppe**.

Zusatzeigenschaften an SharePoint Online Gruppen zuweisen

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

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

Um Zusatzeigenschaften für eine Gruppe festzulegen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > 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.

SharePoint Online Gruppen löschen

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

Um eine Gruppe zu löschen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

SharePoint Online Berechtigungsstufen

Um Berechtigungen auf die Objekte einer Websitesammlung und die darunter liegende Websites zu vergeben, werden in SharePoint Online sogenannte Berechtigungsstufen definiert. Diese Berechtigungsstufen fassen verschiedene, in SharePoint Online fest definierte, Berechtigungen zusammen.

Verwandte Themen

- SharePoint Online Berechtigungsstufen erstellen auf Seite 130
- Stammdaten für SharePoint Online Berechtigungsstufen bearbeiten auf Seite 131
- Stammdaten für SharePoint Online Berechtigungsstufen auf Seite 131
- SharePoint Online Berechtigungsstufen löschen und wiederherstellen auf Seite 132
- Einzelobjekte synchronisieren auf Seite 43

SharePoint Online Berechtigungsstufen erstellen

Um eine Berechtigungsstufe zu erstellen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Berechtigungsstufen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Berechtigungsstufe.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für SharePoint Online Berechtigungsstufen auf Seite 131
- Stammdaten für SharePoint Online Berechtigungsstufen bearbeiten auf Seite 131
- SharePoint Online Berechtigungsstufen löschen und wiederherstellen auf Seite 132

Stammdaten für SharePoint Online Berechtigungsstufen bearbeiten

Um die Stammdaten einer Berechtigungsstufe zu bearbeiten

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Berechtigungsstufen**.
2. Wählen Sie in der Ergebnisliste die Berechtigungsstufe und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten der Berechtigungsstufe.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für SharePoint Online Berechtigungsstufen auf Seite 131
- SharePoint Online Berechtigungsstufen erstellen auf Seite 130
- SharePoint Online Berechtigungsstufen löschen und wiederherstellen auf Seite 132

Stammdaten für SharePoint Online Berechtigungsstufen

Für eine Berechtigungsstufe erfassen Sie die folgenden Stammdaten.

Tabelle 23: Allgemeine Stammdaten einer Berechtigungsstufe

Eigenschaft	Beschreibung
Berechtigungsstufe	Bezeichnung der Berechtigungsstufe.
Websitesammlung	Eindeutige Kennung der Websitesammlung, in der die Berechtigungsstufe angelegt ist.
Berechtigungen	SharePoint Online Berechtigungen, die an die Berechtigungsstufe zugewiesen werden.

Eigenschaft	Beschreibung
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Typ	Typ der Berechtigungsstufe.
Versteckt	Angabe, ob eine SharePoint Online Rolle mit dieser Berechtigungsstufe an Benutzerkonten oder Gruppen zugewiesen werden kann.

Verwandte Themen

- SharePoint Online Berechtigungsstufen auf Seite 130

Überblick über SharePoint Online Berechtigungsstufen

Um einen Überblick über eine Berechtigungsstufe zu erhalten

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Berechtigungsstufen**.
2. Wählen Sie in der Ergebnisliste die Berechtigungsstufe.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Online Berechtigungsstufe**.

SharePoint Online Berechtigungsstufen löschen und wiederherstellen

SharePoint Online 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 im Manager die Kategorie **SharePoint Online > 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 im Manager die Kategorie **SharePoint Online > Berechtigungsstufen**.
2. Wählen Sie in der Ergebnisliste die zum Löschen markierte Berechtigungsstufe.
3. Klicken Sie in der Ergebnisliste .

SharePoint Online Websitesammlungen

Im One Identity Manager werden Websitesammlungen und Websites mit ihren Zugriffsrechten abgebildet. Die 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 Online Rollen, Gruppen und Benutzerkonten in die One Identity Manager-Datenbank eingelesen.

Eine Websitesammlung fasst 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.

Verwandte Themen

- Stammdaten von SharePoint Online Websitesammlungen bearbeiten auf Seite 133
- Einzelobjekte synchronisieren auf Seite 43

Stammdaten von SharePoint Online Websitesammlungen bearbeiten

Um die Stammdaten einer Websitesammlung zu bearbeiten

1. Wählen Sie im Manager die Kategorie **SharePoint Online > 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.

Verwandte Themen

- Allgemeine Stammdaten einer SharePoint Online Websitesammlung auf Seite 134
- Adressdaten einer SharePoint Online Websitesammlung auf Seite 135
- Kategorien für die Vererbung von SharePoint Online Gruppen definieren auf Seite 135

Allgemeine Stammdaten einer SharePoint Online Websitesammlung

Für Websitesammlungen werden die folgende Stammdaten abgebildet.

HINWEIS: Lediglich die Kontendefinition der Websitesammlung kann bearbeitet werden.

Tabelle 24: Allgemeine Stammdaten einer Websitesammlung

Eigenschaft	Beschreibung
Titel	Titel der Websitesammlung.
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.
Mandant	Eindeutige Bezeichnung des Azure Active Directory Mandanten.
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.
Sprachkultur	Name der Sprachkultur, beispielsweise, ES-es.
Zeitzone	Eindeutige Kennung der Zeitzone.
Geolokalisierung	Angaben zur geologischen Lage.
Hauptversion	Die Hauptversion dieser Websitesammlung zum Zweck von Kompatibilitätsprüfungen auf Hauptversionsebene.
Statusinformation	Status der Websitesammlung.
Website-Vorlage	Eindeutige Kennung der SharePoint Online Webvorlage.
Verwendeter Speicherplatz	Information über den Speicherplatz, den die Websitesammlung auf dem Server belegt.
Verwendeter Speicherplatz (%)	Verwendeter Speicherplatz in Prozent.
Maximale Plattengröße	Maximale Speichergröße in Byte, die von dieser Websitesammlung genutzt werden kann.

Eigenschaft	Beschreibung
Warnen ab	Schwellwert in Byte, bei der eine Warnung an den Administrator der Websitesammlung gesendet wird, bevor die maximal verfügbare Speichergröße erreicht ist.
Maximale Anzahl an Zugriffen	Maximale Anzahl an Benutzerzugriffen auf die Websitesammlung pro Tag.
Warnen ab	Schwellwert in Byte, bei der eine Warnung an den Administrator der Websitesammlung gesendet wird, bevor die maximal Anzahl an Benutzerzugriffen auf die Websitesammlung erreicht ist.
Letzte inhalts-relevante Änderung	Zeitpunkt der letzten inhaltsrelevanten Änderung, die an einem Objekt dieser Websitesammlung vorgenommen wurde.

Verwandte Themen

- Kontendefinitionen für SharePoint Online Benutzerkonten auf Seite 51

Adressdaten einer SharePoint Online Websitesammlung

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

Tabelle 25: Adressdaten einer Websitesammlung

Eigenschaften	Beschreibung
URL	Absolute URL der Websitesammlung.
URL relativ zum Server	URL der Websitesammlung, relativ zur URL des Servers.

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

Kategorien für die Vererbung von SharePoint Online Gruppen definieren

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 63**.

Um Kategorien zu definieren

1. Wählen Sie im Manager in der Kategorie **SharePoint Online > 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.

Verwandte Themen

- Vererbung von SharePoint Online Gruppen anhand von Kategorien auf Seite 104

Zusätzliche Aufgaben zur Verwaltung von Websitesammlungen

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

Aufgabe	Thema
Überblick über die SharePoint Online Websitesammlung	Überblick über SharePoint Online Websitesammlungen auf Seite 137
Suchkriterien für die Personenzuordnung definieren	Suchkriterien für die automatische Personenzuordnung bearbeiten auf Seite 74
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 43

Überblick über SharePoint Online Websitesammlungen

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

Um einen Überblick über ein Websitesammlung zu erhalten

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Websitesammlungen**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Online Websitesammlung**.

SharePoint Online Websites

SharePoint Online Websites werden in Websitesammlungen organisiert. Eine Websitesammlung verwaltet Zugriffsrechte und Gestaltungsvorlagen für alle Websites der Websitesammlung. 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.

Verwandte Themen

- Stammdaten von SharePoint Online Websites bearbeiten auf Seite 137
- Einzelobjekte synchronisieren auf Seite 43

Stammdaten von SharePoint Online Websites bearbeiten

Um die Stammdaten einer Website zu bearbeiten

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Websites**.
2. Wählen Sie in der Ergebnisliste die Website.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten von SharePoint Online Websites auf Seite 138
- Adressdaten von SharePoint Online Websites auf Seite 139
- Designinformationen von SharePoint Online Websites auf Seite 140

Allgemeine Stammdaten von SharePoint Online Websites

Für Websites werden die folgenden allgemeine Stammdaten abgebildet.

Tabelle 26: Allgemeine Stammdaten einer Website

Eigenschaft	Beschreibung
Titel	Anzeigename der Website.
Erstellt	Gibt an, wann die Website erstellt wurde.
Version der Benutzeroberfläche	Die Version der Benutzeroberfläche (UI) der Website.
Übergeordnete Website	Eindeutige Kennung der übergeordneten Website.
Websitesammlung	Eindeutige Kennung der Websitesammlung, zu der die Website gehört.
SharePoint Online Websitesammlung	Die übergeordnete Website der gewählten Website.
Sprachkultur	Name der Sprachkultur, beispielsweise, ES-es.
Zeitzone	Eindeutige Kennung der Zeitzone.
Eigene Rollenzuweisungen	Angabe, ob Benutzerkonten oder Gruppen direkt auf die Website berechtigt werden können. Ist die Option deaktiviert, werden die Rollenzuweisungen von der übergeordneten Website geerbt. Es können keine weiteren Benutzerkonten oder Gruppen auf die Website berechtigt werden.
Mitgliedsgruppe	Ermittelt die Benutzer, denen die Berechtigungen für Beiträge auf der Website erteilt wurden.
Eigentümergruppe	Die zugehörigen Eigentümergruppen der Website.
Besuchergruppe	Die zugehörige Besuchergruppe der Website.
Autor	Verweis auf das Benutzerkonto, mit dem die Website erstellt wurde.

Eigenschaft	Beschreibung
E-Mail-Adresse Zugriffsanforderung	E-Mail-Adresse, an die Zugriffsanforderungen gesendet werden.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
RSS-Feeds	Gibt an, ob auf der Website RSS-Feeds zulässig sind.
Enthält vertrauliche Informationen	Angabe, ob die Website vertrauliche Informationen enthält.
Mehrsprachig	Angabe, ob eine mehrsprachige Benutzeroberfläche für die Website aktiviert ist.

Verwandte Themen

- Managen von Zuweisungen von SharePoint Online Gruppen und Rollen auf Seite 89

Adressdaten von SharePoint Online Websites

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

Tabelle 27: Adressdaten einer Website

Eigenschaften	Beschreibung
URL relativ zum Server	URL der Website, relativ zur URL des Servers.
URL	Absolute URL der Website.
URL der System-gestaltungsvorlage	URL zur Systemgestaltungsvorlage, relativ zur URL der Webanwendung.
URL der Gestaltungsvorlage der Website	URL zur Gestaltungsvorlage der Website, relativ zur URL der Webanwendung.

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

Verwandte Themen

- Überblick über SharePoint Online Websites auf Seite 140

Designinformationen von SharePoint Online Websites

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

Tabelle 28: Designinformationen einer Website

Eigenschaft	Beschreibung
Website-Vorlage	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.
URL zum Logo	URL zum Logo der Website, relativ zur URL der Webanwendung.
Beschreibung zum Logo-Icon	Beschreibung zum Logo der Website.

Überblick über SharePoint Online Websites

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 im Manager die Kategorie **SharePoint Online > Websites**.
2. Wählen Sie in der Ergebnisliste die Website.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Online Website**.

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 im Manager die Kategorie **SharePoint Online > Websitesammlungen**.
2. Wählen Sie in der Ergebnisliste die Website.
3. Wählen Sie die Aufgabe **URL öffnen**.

Verwandte Themen

- Adressdaten von SharePoint Online Websites auf Seite 139

Vererbung von SharePoint Online Berechtigungen an untergeordnete SharePoint Online Websites

SharePoint Online 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 Rollenzuweisungen** ist festgelegt, ob Benutzerkonten und Gruppen auf eine Website explizit berechtigt werden können oder ob die Rollenzuweisungen von der übergeordneten Website geerbt werden.

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 Rollenzuweisungen.

   Es gelten sowohl die Berechtigungsstufen und 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 keine Rollenzuweisungen.

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

Verwandte Themen

- Allgemeine Stammdaten von SharePoint Online Websites auf Seite 138
- Managen von Zuweisungen von SharePoint Online Gruppen und Rollen auf Seite 89

SharePoint Online Rollen

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

HINWEIS: SharePoint Online Rollen und Rollenzuweisungen werden bei der Synchronisation als abhängige Objekte behandelt. Das heißt, um Rollenzuweisungen zu synchronisieren, müssen auch die SharePoint Online Rollen synchronisiert werden.

Verwandte Themen

- SharePoint Online Berechtigungsstufen auf Seite 130

Stammdaten für SharePoint Online Rollen bearbeiten

Um die Stammdaten einer SharePoint Online Rolle zu bearbeiten

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Rollen**.
2. Wählen Sie in die Ergebnisliste die SharePoint Online Rolle und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten der Rolle.
4. Speichern Sie die Änderungen.

HINWEIS: Wenn die SharePoint Online 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 Online Rollen können nicht an Benutzerkonten oder Gruppen zugewiesen werden.

Verwandte Themen

- Allgemeine Stammdaten für SharePoint Online Rollen auf Seite 142
- Stammdaten für SharePoint Online Berechtigungsstufen auf Seite 131

Allgemeine Stammdaten für SharePoint Online Rollen

Für SharePoint Online Rollen werden die folgenden Stammdaten abgebildet.

Tabelle 29: Allgemeine Stammdaten einer SharePoint Online Rolle

Eigenschaft	Beschreibung
Anzeigename	Anzeigename der SharePoint Online Rolle.
Berechtigungsstufe	Eindeutige Kennung der Berechtigungsstufe, aus der die SharePoint Online Rolle gebildet ist.

Eigenschaft	Beschreibung
Website	Eindeutige Kennung der Website, an die die SharePoint Online Rolle ihre Berechtigungen vererbt.
Leistungsposition	Angabe einer Leistungsposition, um die Rolle über den IT Shop zu bestellen.
Kategorie	Kategorien für die Vererbung von Rollen. Rollen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Rollen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Shop	Angabe, ob die SharePoint Online Rolle über den IT Shop bestellbar ist. Die SharePoint Online Rolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die SharePoint Online Rolle kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die SharePoint Online Rolle ausschließlich über den IT Shop bestellbar ist. Die SharePoint Online Rolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der SharePoint Online Rolle an hierarchische Rollen ist nicht zulässig.

HINWEIS: Wenn die SharePoint Online 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 Online Rollen können nicht an Benutzerkonten oder Gruppen zugewiesen werden.

Detaillierte Informationen zum Thema

- Stammdaten für SharePoint Online Berechtigungsstufen auf Seite 131

Zusätzliche Aufgaben für die Verwaltung von SharePoint Online Rollen

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

Aufgabe	Thema
Überblick über die SharePoint Online Gruppe	Überblick über SharePoint Online Rollen auf Seite 144

Aufgabe	Thema
Benutzerkonten zuweisen	SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 99
Gruppen zuweisen	SharePoint Online Gruppen an SharePoint Online Rollen zuweisen auf Seite 101
Systemrollen zuweisen	SharePoint Online Berechtigungen in Systemrollen aufnehmen auf Seite 95
Geschäftsrollen zuweisen	SharePoint Online Berechtigungen an Geschäftsrollen zuweisen auf Seite 94
Organisationen zuweisen	SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 93
SharePoint Online Rollen ausschließen	Wirksamkeit von SharePoint Online Rollen auf Seite 144
Zusatzeigenschaften zuweisen	Zusatzeigenschaften an SharePoint Online Gruppen zuweisen auf Seite 129
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 43

Überblick über SharePoint Online Rollen

Um einen Überblick über eine Rolle zu erhalten

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Online Rolle**.

Wirksamkeit von SharePoint Online Rollen

Das unter Wirksamkeit von SharePoint Online Berechtigungszuweisungen auf Seite 102 beschriebene Verhalten können Sie auch für SharePoint Online Rollen nutzen.

Die Wirksamkeit der Zuweisungen wird in den Tabellen `O3SUserHasO3SRLAssign` und `BaseTreeHasO3SRLAssign` über die Spalte `XIsInEffect` abgebildet.

Voraussetzungen

- Der Konfigurationsparameter **QER | Structures | Inherite | GroupExclusion** ist aktiviert.

  Aktivieren Sie im Designer den Konfigurationsparameter und kompilieren Sie die Datenbank.

HINWEIS: Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.

- Sich ausschließende SharePoint Online Rollen gehören zur selben Websitesammlung.

Um SharePoint Online Rollen auszuschließen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **SharePoint Online 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.

Einrichten von SharePoint Online Websitesammlungen und Websites

Websitesammlungen und Websites werden in der Standardinstallation des One Identity Manager durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Über unternehmensspezifische Anpassungen ist es möglich, Websitesammlungen und Websites im One Identity Manager neu anzulegen und in die SharePoint Online-Umgebung zu publizieren. Zu diesem Zweck werden vordefinierte Skripte und Prozesse bereitgestellt. Diese können Sie als Vorlage nutzen, um Websitesammlungen und Websites über den IT Shop bestellbar zu machen.

HINWEIS: Passen Sie die Skripte und Prozesse in jedem Fall unternehmensspezifisch an.

Tabelle 30: Beispielskripte und -prozesse

Skript/Prozess	Beschreibung
Skript `O3S_CreateO3SSite`	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. HINWEIS: Für den Parameter `UID_DialogTimeZone` geben Sie einen für SharePoint Online Zeitzonen zulässigen Wert an. Wenn eine

Skript/Prozess	Beschreibung
	ungültige Zeitzone angegeben wird, wird **UTC** verwendet. Eine Liste der zulässigen Zeitzonen finden Sie im Skriptkommentar.
Skript O3S_CreateO3SWeb	Erstellt eine neue Website innerhalb einer Websitesammlung in der One Identity Manager-Datenbank.
Prozess O3S_O3SWeb_(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. Löscht eine Website. Der Prozess wird durch das Ereignis DEPROVISION ausgelöst, wenn die Website in der One Identity Manager-Datenbank nicht als Root-Site gekennzeichnet ist.
Prozess O3S_O3SSite_(De-)Provision	Erstellt eine neue Websitesammlung innerhalb einer Webanwendung und die zugehörige Root-Site. Der Prozess wird durch das Ereignis PROVISION ausgelöst. Löscht eine Websitesammlung innerhalb einer Webanwendung und die zugehörige Root-Site. Der Prozess wird durch das Ereignis DEPROVISION 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 URL 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.
- Um eine neue Websitesammlung in ein bestehendes Synchronisationsprojekt aufzunehmen, erweitern Sie den Scope der Zielsystemverbindung im Synchronisationsprojekt.

  Scope erweitern

  Der Scope darf nur die Websitesammlungen umfassen, in denen der verwendete Synchronisationsbenutzer in der SharePoint Online Administrationsoberfläche als Websitesammlungsadministrator eingetragen wurde. Es gibt keinen Standardbenutzer in der SharePoint Online-Umgebung.

  Wenn der Scope nicht korrekt eingestellt ist, bricht die Synchronisation beim Laden der zu synchronisierenden Websitesammlungen ab.

Um Websitesammlungen im Scope eines SharePoint Online-Synchronisationsprojektes zu bearbeiten

1. Öffnen Sie den Synchronization Editor.
2. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
3. Wählen Sie die Ansicht **Scope**.
4. Klicken Sie **Scope bearbeiten**. Auf der rechten Seite erscheint eine Liste von Websitesammlungen.
5. Aktivieren Sie die zu synchronisierenden Websitesammlungen.

   Wählen Sie in der Liste der Websitesammlungen nur die, in denen der Synchronisationsbenutzer dem Administrator der SharePoint Online-Umgebung entspricht.
6. Klicken Sie **Übernahme in Datenbank**, um die Änderungen zu speichern.

Ausführliche Informationen zum IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*. Ausführliche Informationen zum Definieren von Prozessen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Verwandte Themen

- Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen auf Seite 30

Berichte über SharePoint Online Objekte

Der One Identity Manager stellt verschiedene Berichte zur Verfügung, in denen Informationen über das ausgewählte Basisobjekt und seine Beziehungen zu anderen Objekten der One Identity Manager-Datenbank aufbereitet sind. Für SharePoint Online stehen folgende Berichte zur Verfügung.

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

Tabelle 31: Berichte zur Datenqualität eines Zielsystems

Bericht	Bereitgestellt für	Beschreibung
Übersicht anzeigen	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Herkunft)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die Herkunft der zugewiesenen Berechtigungen.

Bericht	Bereitgestellt für	Beschreibung
Übersicht anzeigen (inklusive Historie)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Gruppe Rolle	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, welche die ausgewählte Systemberechtigung besitzen.
Übersicht anzeigen	Gruppe Rolle	Der Bericht zeigt einen Überblick über die Systemberechtigung und ihre Zuweisungen.
Übersicht anzeigen (inklusive Herkunft)	Gruppe Rolle	Der Bericht zeigt einen Überblick über die Systemberechtigung und die Herkunft der zugewiesenen Benutzerkonten.
Übersicht anzeigen (inklusive Historie)	Gruppe Rolle	Der Bericht zeigt einen Überblick über die Systemberechtigung einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Benutzerkonten anzeigen (inklusive Historie)	Websitesammlung Website	Der Bericht liefert alle Benutzerkonten mit ihren Berechtigungen einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Systemberechtigungen anzeigen (inklusive Historie)	Websitesammlung Website	Der Bericht zeigt die Systemberechtigungen mit den zugewiesenen Benutzerkonten einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die

Bericht	Bereitgestellt für	Beschreibung
		Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Websitesammlung Mandant	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Zielsystem mindestens ein Benutzerkonto besitzen.

Behandeln von SharePoint Online Objekten im Web Portal

Der One Identity Manager bietet seinen Benutzern die Möglichkeit, verschiedene Aufgaben unkompliziert über ein Web Portal zu erledigen.

- Managen von Benutzerkonten und Personen

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

- Managen von Berechtigungszuweisungen

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

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

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

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

- Attestierung

  Dafür werden im Manager Attestierungsrichtlinien konfiguriert. Die Attestierer nutzen das Web Portal, um Attestierungsvorgänge zu entscheiden.

- Governance Administration

  Die Regeln werden regelmäßig und bei Änderungen an den Objekten im One Identity Manager überprüft. Complianceregeln werden im Manager definiert. Verantwortliche Personen nutzen das Web Portal, um Regelverletzungen zu überprüfen, aufzulösen und Ausnahmegenehmigungen zu erteilen.

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

- Risikobewertung

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

- Berichte und Statistiken

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

Ausführliche Informationen zu den genannten Themen finden Sie in folgenden Handbüchern:

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

Basisdaten für die Verwaltung einer SharePoint Online-Umgebung

Für die Verwaltung einer SharePoint Online-Umgebung im One Identity Manager sind folgende Basisdaten relevant.

- Authentifizierungsmodi

  Authentifizierungsmodus, der bei der Anmeldung mit diesem Benutzerkonto am SharePoint Online Server genutzt wird. Für SharePoint Online gilt **AzureAD** als einziger Authentifizierungsmodus.

  Weitere Informationen finden Sie unter SharePoint Online Authentifizierungsmodi auf Seite 153.

- Zielsystemtypen

  Zielsystemtypen werden für die Konfiguration des Zielsystemabgleichs benötigt. An den Zielsystemtypen werden die Tabellen gepflegt, die ausstehende Objekte enthalten können. Es werden Einstellungen für die Provisionierung von Mitgliedschaften und die Einzelobjektsynchronisation vorgenommen. Zusätzlich dient der Zielsystemtyp zur Abbildung der Objekte im Unified Namespace.

  Weitere Informationen finden Sie unter Ausstehende Objekte nachbehandeln auf Seite 45.

- Kontendefinitionen

  Um 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 Kontendefinitionen für SharePoint Online Benutzerkonten auf Seite 51.

- Server

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

  Weitere Informationen finden Sie unter Jobserver für SharePoint Online-spezifische Prozessverarbeitung auf Seite 154.

- Zielsystemverantwortliche

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

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

Weitere Informationen finden Sie unter Zielsystemverantwortliche auf Seite 159.

SharePoint Online Authentifizierungsmodi

Um die Stammdaten für einen Authentifizierungsmodus anzuzeigen

1. Wählen Sie im Manager die Kategorie **SharePoint Online > Basisdaten zur Konfiguration > Authentifizierungsmodi**.
2. Wählen Sie in der Ergebnisliste den Authentifizierungsmodus.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Für den Authentifizierungsmodus werden folgende Stammdaten geliefert.

Tabelle 32: Eigenschaften eines Authentifizierungsmodus

Eigenschaft	Beschreibung
System ID	Bezeichnung des Authentifizierungsmodus. Für SharePoint Online gilt **AzureAD** als einziger 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.

SharePoint Online Webvorlagen

Um Websites und Websitesammlungen im One Identity Manager anlegen zu können, werden Webvorlagen in den One Identity Manager eingelesen.

Um einen Überblick über eine Webvorlage zu erhalten

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

Verwandte Themen

- Einrichten von SharePoint Online Websitesammlungen und Websites auf Seite 145

Jobserver für SharePoint Online-spezifische Prozessverarbeitung

Für die Verarbeitung der zielsystemspezifischen 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 Online > 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.

Um einen Jobserver und seine Funktionen zu bearbeiten

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Jobserver auf Seite 155
- Festlegen der Serverfunktionen auf Seite 157

Verwandte Themen

- Systemanforderungen für den SharePoint Online Synchronisationsserver auf Seite 18

Allgemeine Stammdaten für Jobserver

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

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

Tabelle 33: Eigenschaften eines Jobservers

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS Syntax. Syntax: `<Name des Servers>.<Vollqualifizierter Domänenname>`
Server ist Cluster	Gibt an, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. HINWEIS: Die Eigenschaften **Server ist Cluster** und **Server gehört zu Cluster** schließen einander aus.
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.
IP-Adresse (IPv4)	Internet Protokoll Version 4 (IPv4)-Adresse des Servers.
Kopierverfahren (Zielserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Ziel einer Kopieraktion ist.
Codierung	Codierung des Zeichensatzes mit der Dateien auf dem Server geschrieben werden.
Übergeordneter Jobserver	Bezeichnung des übergeordneten Jobservers.
Ausführender Server	Bezeichnung des ausführenden Servers. Eingetragen wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden.

Eigenschaft	Bedeutung
	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. Mit dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Serverbetriebssystem	Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte **Win32**, **Windows**, **Linux** und **Unix**. Ist die Angabe leer, wird **Win32** angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen.
One Identity Manager Service installiert	Gibt an, 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	Gibt an, 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 Berechtigungen im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*.
Kein automatisches Softwareupdate	Gibt an, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.

Eigenschaft	Bedeutung
Softwareupdate läuft	Gibt an, ob gerade eine Softwareaktualisierung ausgeführt wird.
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 157

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 34: Zulässige Serverfunktionen

Serverfunktion	Anmerkungen
Azure Active Directory Konnektor (via Microsoft Graph)	Server, auf dem der Azure Active Directory Konnektor installiert ist. Der Server führt die Synchronisation mit dem Zielsystem Azure 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.

Serverfunktion	Anmerkungen
	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.
Generischer Datenbankkonnektor	Der Server kann sich mit einer ADO.Net Datenbank verbinden.
One Identity Manager-Datenbankkonnektor	Server, auf dem der One Identity Manager Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem One Identity Manager aus.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
Primärer Domänen-Controller	Primärer Domänen-Controller.
Profilserver	Server für die Einrichtung von Profilverzeichnissen für Benutzerkonten.
SAM Synchronisationsserver	Server für die Synchronisation mit einem SMB-basierten Zielsystem aus.
SharePoint Online Konnektor	Server, auf dem der SharePoint Online Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem SharePoint Online 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.
SCIM Konnektor	Der Server kann sich mit einer Cloud-Anwendung verbinden.

Verwandte Themen

- Allgemeine Stammdaten für Jobserver auf Seite 155

Zielsystemverantwortliche

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

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

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

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

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

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

Tabelle 35: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | SharePoint Online** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**.

Benutzer	Aufgaben
	• 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 Online**.
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 Online > Basisdaten zur Konfiguration > Zielsystemverantwortliche** die Anwendungsrolle.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Personen zu und speichern Sie die Änderungen.

Um Zielsystemverantwortliche für einzelne Mandanten festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **SharePoint Online > Mandanten**.
3. Wählen Sie in der Ergebnisliste den Mandanten.

4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Zielsystemverantwortliche** die Anwendungsrolle.

   - ODER -

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

   a. Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Zielsysteme | SharePoint Online** zu.

   b. Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.
6. Speichern Sie die Änderungen.
7. Weisen Sie der Anwendungsrolle die Personen zu, die berechtigt sind, den Mandanten im One Identity Manager zu bearbeiten.

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer SharePoint Online-Umgebung auf Seite 9

Beheben von Fehlern beim Anbinden einer SharePoint Online-Umgebung

Synchronisationsfehler nach Umbenennung einer SharePoint Online Websitesammlung

Nachdem eine Websitesammlung, die bereits in die One Identity Manager-Datenbank eingelesen wurde, in der SharePoint Online-Umgebung umbenannt wurde, bricht die Synchronisation mit einer Fehlermeldung ab.

Wahrscheinliche Ursache

Im Scope des Synchronisationsprojekts ist noch der alte Titel der Websitesammlung referenziert.

Lösung

- Korrigieren Sie den Scope des Synchronisationsprojekts und wählen Sie die Websitesammlung, deren URL den neuen Titel enthält.

Verwandte Themen

- Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen auf Seite 30

Anhang A

Konfigurationsparameter für die Verwaltung einer SharePoint Online

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

Tabelle 36: Konfigurationsparameter

Konfigurationsparameter	Bedeutung
TargetSystem | SharePointOnline	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung des Zielsystems SharePoint Online. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
TargetSystem | SharePointOnline | Accounts	Parameter zur Konfiguration der Angaben zu SharePoint Online Benutzerkonten.
TargetSystem | SharePointOnline | Accounts | MailTemplateDefaultValues	Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto mit Standardwerten** verwendet.
TargetSystem | SharePointOnline | DefaultAddress	Standard-E-Mail-Adresse des Empfängers von Benachrichtigungen über Aktionen im Zielsystem.

Konfigurationsparameter	Bedeutung
TargetSystem | SharePointOnline | MaxFullsyncDuration	Maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.
TargetSystem | SharePointOnline | PersonAutoDefault	Modus für die automatische Personenzuordnung für Benutzerkonten, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem | SharePointOnline | PersonAutoFullsync	Modus für die automatische Personenzuordnung für Benutzerkonten, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.

Anhang B

Standardprojektvorlage für SharePoint Online

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.

HINWEIS: Es gibt nur eine Synchronisationsvorlage im One Identity Manager für das Zielsystem SharePoint Online.

Für die Synchronisation von Benutzerkonten und Berechtigungen einer SharePoint Online nutzen Sie die Projektvorlage **SharePoint Online Synchronisation**. Die Projektvorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 37: Abbildung der SharePoint Online Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im SharePoint Online	Tabelle im One Identity Manager Schema
Tenant	O3STenant
Site	O3SSite
Group	O3SGroup
Web	O3SWeb
RoleAssignment	O3SRLAsgn
RoleDefinition	O3SRole
User	O3SUser
WebTemplate	O3SWebTemplate

Anhang C

Verarbeitung von Systemobjekten

Folgende Tabelle beschreibt die zulässigen Verarbeitungsmethoden für die Schematypen der SharePoint Online und benennt notwendige Einschränkungen bei der Verarbeitung der Systemobjekte im Manager.

Tabelle 38: Zulässige Verarbeitungsmethoden für Objekttypen

Typ	Lesen	Hinzufügen	Löschen	Ändern
Mandant	Ja	Nein	Nein	Nein
Websitesammlung	Ja	(Ja)	(Ja)	Nein
Benutzerkonto	Ja	Ja	Ja	Ja
Gruppe	Ja	Ja	Ja	Ja
Website	Ja	(Ja)	(Ja)	Ja
Rolle	Ja	Ja	Ja	Ja
Rollenzuweisung	Ja	Nein	Nein	Ja

(Ja): Es ist technisch möglich, Websitesammlungen und Websites anzulegen und zu löschen. Die dafür benötigten Skripte und Prozesse müssen jedoch unternehmensspezifisch eingerichtet werden. Weitere Informationen finden Sie unter Einrichten von SharePoint Online Websitesammlungen und Websites auf Seite 145.

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

G

I

J

K

L

M

N

O

P

R

S

U

V

W

Z