



One Identity Manager 8.1.2

Administrationshandbuch für die
Anbindung einer SharePoint Online-
Umgebung

Copyright 2020 One Identity LLC.

ALLE RECHTE VORBEHALTEN.

Diese Anleitung enthält urheberrechtlich geschützte Informationen. Die in dieser Anleitung beschriebene Software wird unter einer Softwarelizenz oder einer Geheimhaltungsvereinbarung bereitgestellt. Diese Software darf nur in Übereinstimmung mit den Bestimmungen der geltenden Vereinbarung verwendet oder kopiert werden. Kein Teil dieser Anleitung darf ohne die schriftliche Erlaubnis von One Identity LLC in irgendeiner Form oder mit irgendwelchen Mitteln, elektronisch oder mechanisch reproduziert oder übertragen werden, einschließlich Fotokopien und Aufzeichnungen für irgendeinen anderen Zweck als den persönlichen Gebrauch des Erwerbers.

Die Informationen in diesem Dokument werden in Verbindung mit One Identity Produkten bereitgestellt. Durch dieses Dokument oder im Zusammenhang mit dem Verkauf von One Identity LLC Produkten wird keine Lizenz, weder ausdrücklich oder stillschweigend, noch durch Duldung oder anderweitig, an jeglichem geistigen Eigentumsrecht eingeräumt. MIT AUSNAHME DER IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT GENANNTEN BEDINGUNGEN ÜBERNIMMT ONE IDENTITY KEINERLEI HAFTUNG UND SCHLIESST JEGLICHE AUSDRÜCKLICHE, IMPLIZIERTE ODER GESETZLICHE GEWÄHRLEISTUNG ODER GARANTIE IN BEZUG AUF IHRE PRODUKTE AUS, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE IMPLIZITE GEWÄHRLEISTUNG DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET ONE IDENTITY FÜR JEGLICHE DIREKTE, INDIREKTE, FOLGE-, STÖRUNGS-, SPEZIELLE ODER ZUFÄLLIGE SCHÄDEN (EINSCHLIESSLICH, OHNE EINSCHRÄNKUNG, SCHÄDEN FÜR VERLUST VON GEWINNEN, GESCHÄFTSUNTERBRECHUNGEN ODER VERLUST VON INFORMATIONEN), DIE AUS DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DIESES DOKUMENTS RESULTIEREN, SELBST WENN ONE IDENTITY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN HAT. One Identity übernimmt keinerlei Zusicherungen oder Garantien hinsichtlich der Richtigkeit und Vollständigkeit des Inhalts dieses Dokuments und behält sich das Recht vor, Änderungen an Spezifikationen und Produktbeschreibungen jederzeit ohne vorherige Ankündigung vorzunehmen. One Identity verpflichtet sich nicht, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Wenn Sie Fragen zu Ihrer potenziellen Nutzung dieses Materials haben, wenden Sie sich bitte an:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Besuchen Sie unsere Website (<http://www.OneIdentity.com>) für regionale und internationale Büro-Adressen.

Patente

One Identity ist stolz auf seine fortschrittliche Technologie. Für dieses Produkt können Patente und anhängige Patente gelten. Für die aktuellsten Informationen über die geltenden Patente für dieses Produkt besuchen Sie bitte unsere Website unter <http://www.OneIdentity.com/legal/patents.aspx>.

Marken

One Identity und das One Identity Logo sind Marken und eingetragene Marken von One Identity LLC. in den USA und anderen Ländern. Für eine vollständige Liste der One Identity Marken besuchen Sie bitte unsere Website unter www.OneIdentity.com/legal. Alle anderen Marken sind Eigentum der jeweiligen Besitzer.

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.

Inhalt

Abbilden einer SharePoint Online-Umgebung im One Identity Manager	8
Architekturüberblick	8
One Identity Manager Benutzer für die Verwaltung einer SharePoint Online-Umgebung	9
Konfigurationsparameter	11
Synchronisieren einer SharePoint Online-Umgebung	12
Einrichten der Initialsynchronisation	12
Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung	13
Einrichten des SharePoint Online Synchronisationservers	15
Systemanforderungen für den Synchronisationsserver	15
One Identity Manager Service installieren	16
Vorbereiten eines Remoteverbindungsservers für den Zugriff auf den SharePoint Online Mandanten	19
Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines SharePoint Online Mandanten	20
Benötigte Informationen für die Erstellung eines Synchronisationsprojektes	20
Initiales Synchronisationsprojekt für SharePoint Online erstellen	21
Synchronisationsprotokoll konfigurieren	25
Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen	26
Anpassen einer Synchronisationskonfiguration	26
Synchronisation in den SharePoint Online Mandanten konfigurieren	28
Schema aktualisieren	28
Provisionierung von Mitgliedschaften konfigurieren	29
Einzelobjektsynchronisation konfigurieren	31
Beschleunigung der Provisionierung und Einzelobjektsynchronisation	32
Ausführen einer Synchronisation	33
Synchronisationen starten	34
Synchronisationsergebnisse anzeigen	35
Synchronisation deaktivieren	36
Einzelobjekte synchronisieren	36
Aufgaben nach einer Synchronisation	37
Ausstehende Objekte nachbehandeln	37

Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen	39
Benutzerkonten über Kontendefinitionen verwalten	40
Fehleranalyse	40
Managen von SharePoint Online Benutzerkonten und Personen	42
Kontendefinitionen für SharePoint Online Benutzerkonten	43
Kontendefinitionen erstellen	44
Kontendefinitionen bearbeiten	44
Stammdaten von Kontendefinitionen	44
Automatisierungsgrade bearbeiten	47
Automatisierungsgrade erstellen	48
Stammdaten von Automatisierungsgraden	48
Abbildungsvorschriften für IT Betriebsdaten erstellen	50
IT Betriebsdaten erfassen	51
IT Betriebsdaten ändern	53
Zuweisen der Kontendefinition an Personen	54
Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen	55
Kontendefinitionen an Geschäftsrollen zuweisen	55
Kontendefinitionen an alle Personen zuweisen	56
Kontendefinitionen direkt an Personen zuweisen	56
Kontendefinitionen an Systemrollen zuweisen	57
Kontendefinitionen in den IT Shop aufnehmen	57
Kontendefinitionen an Zielsysteme zuweisen	59
Kontendefinitionen löschen	59
Automatische Zuordnung von Personen zu SharePoint Online Benutzerkonten	62
Suchkriterien für die automatische Personenzuordnung bearbeiten	63
Personen suchen und direkt an Benutzerkonten zuordnen	65
Automatisierungsgrad an SharePoint Online Benutzerkonten ändern	66
Kontendefinitionen an verbundene SharePoint Online Benutzerkonten zuweisen	67
Personen manuell mit SharePoint Online Benutzerkonten verbinden	68
Anwendungsfälle für SharePoint Online Benutzerkonten	68
Unterstützte Typen von Benutzerkonten	70
Standardbenutzerkonten	71
Administrative Benutzerkonten	72
Administrative Benutzerkonten für eine Person bereitstellen	73
Administrative Benutzerkonten für mehrere Personen bereitstellen	74

Privilegierte Benutzerkonten	75
Managen von Zuweisungen von SharePoint Online Gruppen und Rollen	78
Zuweisen von SharePoint Online Berechtigungen an SharePoint Online Benutzerkonten im One Identity Manager	79
SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen	80
SharePoint Online Berechtigungen an Geschäftsrollen zuweisen	82
SharePoint Online Berechtigungen in Systemrollen aufnehmen	83
SharePoint Online Berechtigungen in den IT Shop aufnehmen	84
SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen	86
SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen	87
SharePoint Online Rollen an SharePoint Online Gruppen zuweisen	87
SharePoint Online Gruppen an SharePoint Online Rollen zuweisen	88
Wirksamkeit von SharePoint Online Berechtigungszuweisungen	89
Vererbung von SharePoint Online Gruppen anhand von Kategorien	91
Übersicht aller Zuweisungen	94
Abbilden von SharePoint Online Objekten im One Identity Manager	96
SharePoint Online Mandanten	96
Allgemeine Stammdaten für SharePoint Online Mandanten	97
Zusätzliche Aufgaben zur Verwaltung von SharePoint Online Mandanten	98
Überblick über einen SharePoint Online Mandanten	99
Synchronisationsprojekt für einen SharePoint Online Mandanten bearbeiten	99
SharePoint Online Benutzerkonten	100
SharePoint Online Benutzerkonten erstellen	101
Stammdaten für SharePoint Online Benutzerkonten bearbeiten	101
Erfassen der Stammdaten für SharePoint Online Benutzerkonten	102
Stammdaten eines benutzerauthentifizierten Benutzerkontos	102
Stammdaten eines gruppenauthentifizierten Benutzerkontos	105
Zusätzliche Aufgaben zur Verwaltung von SharePoint Online Benutzerkonten	108
Überblick über ein SharePoint Online Benutzerkonto	108
Zusatzeigenschaften zuweisen	109
SharePoint Online Benutzerkonten löschen und wiederherstellen	109
SharePoint Online Gruppen	110
SharePoint Online Gruppen erstellen	111
Stammdaten für SharePoint Online Gruppen bearbeiten	112

Stammdaten für SharePoint Online Gruppen	112
Zusätzliche Aufgaben zur Verwaltung von SharePoint Online Gruppen	114
Überblick über SharePoint Online Gruppen	114
Zusatzeigenschaften an SharePoint Online Gruppen zuweisen	115
SharePoint Online Gruppen löschen	115
SharePoint Online Berechtigungsstufen	115
SharePoint Online Berechtigungsstufen erstellen	116
Stammdaten für SharePoint Online Berechtigungsstufen bearbeiten	116
Allgemeine Stammdaten für SharePoint Online Berechtigungsstufen	117
Überblick über SharePoint Online Berechtigungsstufen	117
Löschen von SharePoint Online Berechtigungsstufen	117
SharePoint Online Websitesammlungen	118
Allgemeine Stammdaten einer SharePoint Online Websitesammlung	119
Adressdaten einer SharePoint Online Websitesammlung	120
Festlegen der Kategorien für die Vererbung von SharePoint Online Gruppen	120
Zusätzliche Aufgaben zur Verwaltung von Websitesammlungen	121
Überblick über eine SharePoint Online Websitesammlung	121
SharePoint Online Websites	122
Allgemeine Stammdaten von SharePoint Online Websites	122
Adressdaten von SharePoint Online Websites	123
Designinformationen von SharePoint Online Websites	124
Überblick über SharePoint Online Websites	124
Vererbung von SharePoint Online Berechtigungen an untergeordnete SharePoint Online Websites	125
SharePoint Online Rollen	126
Stammdaten für SharePoint Online Rollen bearbeiten	126
Allgemeine Stammdaten für SharePoint Online Rollen	127
Zusätzliche Aufgaben für die Verwaltung von SharePoint Online Rollen	128
Überblick über eine SharePoint Online Rolle	128
Wirksamkeit von SharePoint Online Rollen	129
Behandeln von SharePoint Online Objekten im Web Portal	130
Basisdaten für die Verwaltung einer SharePoint Online-Umgebung	132
SharePoint Online Authentifizierungsmodi	133
Jobserver für SharePoint Online-spezifische Prozessverarbeitung	133
SharePoint Online Jobserver bearbeiten	134

Stammdaten eines Jobserverns	135
Festlegen der Serverfunktionen	137
Zielsystemverantwortliche	139
Anhang: Konfigurationsparameter für die Verwaltung einer SharePoint Online	142
Anhang: Standardprojektvorlage für SharePoint Online	144
Anhang: Verarbeitung von Systemobjekten	145
Über uns	146
Kontaktieren Sie uns	146
Technische Supportressourcen	146
Index	147

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 145

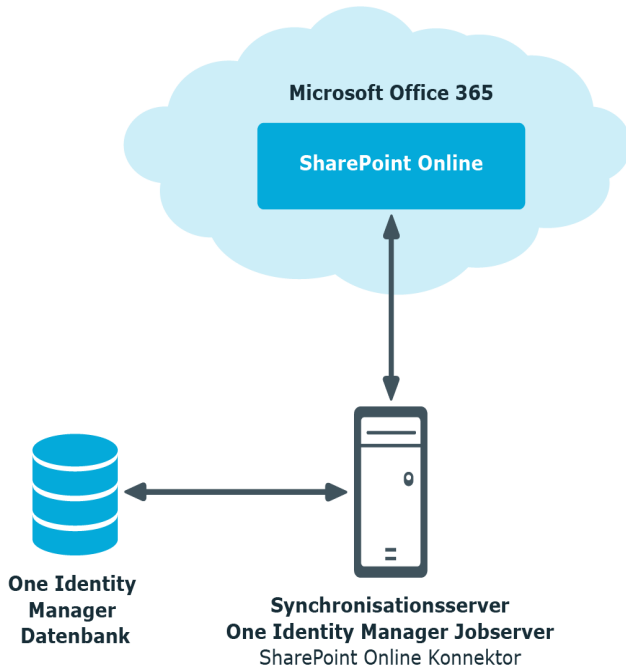
Architekturüberblick

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 MicrosoftOffice 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, wie beispielsweise Benutzerkonten oder Gruppen.
- 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

- Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen.

- Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen.
- Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter.
- Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse.
- Erstellen und konfigurieren bei Bedarf Zeitpläne.
- Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.

Konfigurationsparameter

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

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

Weitere Informationen finden Sie unter [Konfigurationsparameter für die Verwaltung einer SharePoint Online](#) auf Seite 142.

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](#) auf Seite 12
- [Anpassen einer Synchronisationskonfiguration](#) auf Seite 26
- [Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen](#) auf Seite 26
- [Ausführen einer Synchronisation](#) auf Seite 33
- [Fehleranalyse](#) auf Seite 40
- [Verarbeitung von Systemobjekten](#) auf Seite 145

Einrichten der Initialsynchronisation

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. 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.
 - Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.
3. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
4. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Detaillierte Informationen zum Thema

- [Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung](#) auf Seite 13
- [Systemanforderungen für den Synchronisationsserver](#) auf Seite 15
- [Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines SharePoint Online Mandanten](#) auf Seite 20
- [Konfigurationsparameter für die Verwaltung einer SharePoint Online](#) auf Seite 142
- [Standardprojektvorlage für SharePoint Online](#) auf Seite 144

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	<p>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:</p> <ul style="list-style-type: none"> • ein administratives Benutzerkonto des zugehörigen Azure Active Directory Mandanten, welches eine der folgenden Administratorrollen besitzt. <ul style="list-style-type: none"> • SharePoint Administratoren • Azure Active Directory Unternehmensadministrator/Globaler Administrator <p>HINWEIS: Dieses Benutzerkonto muss an allen zu administrierenden Websitesammlungen als Websitesammlungsadministrator eingetragen werden. Dies nehmen Sie im SharePoint Online vor.</p> <p>Ausführliche Informationen zu Websitesammlungsadministratoren finden Sie in der Dokumentation von Microsoft.</p>
Benutzerkonto des One Identity Manager Service	<p>Das Benutzerkonto für den One Identity Manager Service benötigt die Rechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Rechte vergeben, Verzeichnisse und Dateien anlegen und bearbeiten.</p> <p>Das Benutzerkonto muss der Gruppe Domänen-Benutzer angehören.</p> <p>Das Benutzerkonto benötigt das erweiterte Benutzerrecht Anmelden als Dienst.</p> <p>Das Benutzerkonto benötigt Rechte für den internen Webservice.</p> <p>HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (NT Authority\NetworkService) laufen, so können Sie die Rechte für den internen Webservice über folgenden Kommandozeilenaufruf vergeben:</p> <pre>netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis.</p> <p>In der Standardinstallation wird der One Identity Manager installiert unter:</p> <ul style="list-style-type: none"> • %ProgramFiles(x86)%\One Identity (auf 32-Bit Betriebssystemen) • %ProgramFiles%\One Identity (auf 64-Bit Betriebssystemen)

Benutzer	Berechtigungen
Benutzer für den Zugriff auf die One Identity Manager-Datenbank	Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer Synchronization bereitgestellt.

Einrichten des 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.

Detaillierte Informationen zum Thema

- [Systemanforderungen für den Synchronisationsserver](#) auf Seite 15
- [One Identity Manager Service installieren](#) auf Seite 16

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

| **HINWEIS:** Beachten Sie die Empfehlungen des Zielsystemherstellers.

One Identity Manager Service installieren

Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem SharePoint Online Konnektor installiert sein. Außerdem muss der Synchronisationsserver 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: Für die Generierung von Prozessen für die Jobserver werden der Provider, Verbindungsparameter und die Authentifizierungsdaten benötigt. Diese Informationen werden im Standardfall aus den Verbindungsdaten der Datenbank ermittelt. Arbeitet der Jobserver über einen Anwendungsserver müssen Sie zusätzliche Verbindungsinformationen im Designer konfigurieren. Ausführliche Informationen zum Einrichten des Jobservers finden Sie im *One Identity Manager Konfigurationshandbuch*.

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

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

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

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

- a. Wählen Sie in der Auswahlliste **Server** einen Jobserver aus.
- ODER -

Um einen neuen Jobserver zu erstellen, klicken Sie **Hinzufügen**.

- b. Bearbeiten Sie folgende Informationen für den Jobserver.
 - **Server**: Bezeichnung des Jobservers.
 - **Queue**: Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
 - **Vollständiger Servername**: Vollständiger Servername gemäß DNS Syntax.

Syntax:

<Name des Servers>.<Vollqualifizierter Domänenname>

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

4. Auf der Seite **Maschinenrollen** wählen Sie **SharePoint 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:
 - a. Wählen Sie **Prozessabholung | sqlprovider**
 - b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
 - c. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
- Für eine Verbindung zum Anwendungsserver:

- a. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
 - b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
 - c. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.
 - d. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
 - e. Wählen Sie das Authentifizierungsmodul. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
7. Zur Konfiguration der Remote-Installation, klicken Sie **Weiter**.
 8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
 9. Auf der Seite **Installationsquelle festlegen** wählen Sie das Verzeichnis mit den Installationsdateien.
 10. Auf der Seite **Datenbankschlüsseldatei auswählen** wählen die Datei mit dem privaten Schlüssel.
| **HINWEIS:** Diese Seite wird nur angezeigt, wenn die Datenbank verschlüsselt ist.
 11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
 - **Computer:** Name oder IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
 - **Dienstkonto:** Angaben zum Benutzerkonto des One Identity Manager Service.
 - Um den Dienst unter einem anderen Konto zu starten, deaktivieren Sie die Option **Lokales Systemkonto** und erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung.
 - **Installationskonto:** Angaben zum administrativen Benutzerkonto für die Installation des Dienstes.
 - Um das Benutzerkonto des angemeldeten Benutzers zu verwenden, aktivieren Sie die Option **Angemeldeter Benutzer**.
 - Um ein anderes Benutzerkonto zu verwenden, deaktivieren Sie die Option **Angemeldeter Benutzer** und geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.
 - Um das Installationsverzeichnis, den Namen, den Anzeigenamen oder die Beschreibung für den One Identity Manager Service zu ändern, nutzen Sie die weiteren Optionen.
 12. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.
Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.
 13. Auf der letzten Seite des Server Installer klicken Sie **Fertig**.

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

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 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 15
- [Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung](#) auf Seite 13

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 Basisdomäne	Bezeichnung der Azure Active Directory Basisdomäne ohne .onmicrosoft.com.
Benutzername und Kennwort zur Anmeldung	Benutzerkonto und Kennwort zur Authentifizierung am SharePoint Online. 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 13.
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

Angaben

Erläuterungen

installiert sein.

Tabelle 5: Eigenschaften des Jobserver

Eigenschaft	Wert
Serverfunktion	SharePoint Online Konnektor
Maschinenrolle	Server Jobserver SharePoint Online

Weitere Informationen finden Sie unter [Einrichten des SharePoint Online Synchronisationsservers](#) auf Seite 15.

Verbindungsdaten zur One Identity Manager-Datenbank

- Datenbankserver
- Datenbank
- SQL Server Anmeldung und Kennwort
- Angabe, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.

Remoteverbindungsserver

Weitere Informationen finden Sie unter [Vorbereiten eines Remoteverbindungservers für den Zugriff auf den SharePoint Online Mandanten](#) auf Seite 19.

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.

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 folgenden Anmeldeinformationen für die Verbindung zum SharePoint Online.

- **Basisdomäne:** Erfassen Sie die Bezeichnung der Azure Active Directory Basisdomäne ohne .onmicrosoft.com.
- **Benutzername:** Erfassen Sie den vollqualifizierter Namen (FQDN) des Benutzerkontos zur Anmeldung am SharePoint Online in der Form user@domain.

Beispiel:

<Benutzername des Synchronisationsnutzers>@yourorganization.onmicrosoft.com

- **Kennwort:** Erfassen Sie das Kennwort zum Benutzerkonto.
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 Zielsystemschemata. 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.	<p>Angabe, ob nur ein Synchronisationsworkflow zum initialen Einlesen des Zielsystems in die One Identity Manager-Datenbank eingerichtet werden soll.</p> <p>Der Synchronisationsworkflow zeigt folgende Besonderheiten:</p> <ul style="list-style-type: none">• 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.	<p>Angabe, ob zusätzlich zum Synchronisationsworkflow zum initialen Einlesen des Zielsystems ein Provisionierungsworkflow eingerichtet werden soll.</p> <p>Der Provisionierungsworkflow zeigt folgende Besonderheiten:</p> <ul style="list-style-type: none">• 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 Jobserver und den vollständigen Servernamen gemäß DNS-Syntax.
- c. Klicken Sie **OK**.

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

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

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**.

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

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 auszuschließen

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. 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 Ihre Änderungen zu speichern.

Verwandte Themen

- [Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung](#) auf Seite 13
- [Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen](#) auf Seite 26
- [Einrichten des SharePoint Online Synchronisationservers](#) auf Seite 15
- [Synchronisationsprotokoll konfigurieren](#) auf Seite 25
- [Anpassen einer Synchronisationskonfiguration](#) auf Seite 26

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 35

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 Zielsystemschemata 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 auszuschließen

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. 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 Ihre Änderungen zu speichern.

Verwandte Themen

- [Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung](#) auf Seite 13

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 Mastersystem 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 Zielsystemschemata geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.
- Um zusätzliche Schemaeigenschaften zu synchronisieren, aktualisieren Sie das Schema im Synchronisationsprojekt. Nehmen Sie die Schemaerweiterungen in das Mapping auf.
- Um Daten zu synchronisieren, für die keine Schematypen im Konnektorschema angelegt sind, legen Sie eigene Schematypen an. Nehmen Sie die Schemaerweiterungen in das Mapping auf.

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

Detaillierte Informationen zum Thema

- [Synchronisation in den SharePoint Online Mandanten konfigurieren](#) auf Seite 28
- [Schema aktualisieren](#) auf Seite 28
- [Provisionierung von Mitgliedschaften konfigurieren](#) auf Seite 29
- [Einzelobjektsynchronisation konfigurieren](#) auf Seite 31
- [Beschleunigung der Provisionierung und Einzelobjektsynchronisation](#) auf Seite 32

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 Mastersystem 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 das Synchronisationsprojekt im Synchronization Editor.
2. Prüfen Sie, ob die bestehenden Mappings für die Synchronisation in das Zielsystem genutzt werden können. Erstellen Sie bei Bedarf neue Mappings.
3. Erstellen Sie mit dem Workflowassistenten einen neuen Workflow.
Es wird ein Workflow mit der Synchronisationsrichtung **In das Zielsystem** angelegt.
4. Erstellen Sie eine neue Startkonfiguration. Nutzen Sie dabei den neu angelegten Workflow.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

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 Zielsystemschemata 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 Zielsystemschemata
 - 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. Wählen Sie die Kategorie **Konfiguration | Zielsystem**.
- ODER -
Wählen Sie die Kategorie **Konfiguration | One Identity Manager Verbindung**.
2. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
3. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
Die Schemadaten werden neu geladen.

Um ein Mapping zu bearbeiten

1. Wählen Sie die Kategorie **Mappings**.
2. Wählen Sie in der Navigationsansicht das Mapping.
Der Mappingeditor wird geöffnet. Ausführliche Informationen zum Bearbeiten von Mappings finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

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

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 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.
 - Die Option kann nur für Zuordnungstabellen aktiviert werden, deren Basistabelle eine Spalte `XDateSubItem` oder `CCC_XDateSubItem` hat.
 - Zuordnungstabellen, die im Mapping in einer virtuellen Schemaeigenschaft zusammengefasst sind, müssen identisch markiert werden.
5. Klicken Sie **Änderungen zusammenführen**.
6. Speichern Sie die Änderungen.

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

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

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

Um die Standardbedingung wiederherzustellen

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

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

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_03STenant).XObjectKey
8. Speichern Sie die Änderungen.

Verwandte Themen

- [Einzelobjekte synchronisieren](#) auf Seite 36
- [Ausstehende Objekte nachbehandeln](#) auf Seite 37

Beschleunigung der Provisionierung und Einzelobjektsynchronisation

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

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

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

Um die Lastverteilung zu konfigurieren

1. Konfigurieren Sie die Server und geben Sie diese im One Identity Manager als Jobserver bekannt.
 - Weisen Sie diesen Jobservern die Serverfunktion **SharePoint 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

- [SharePoint Online Jobserver bearbeiten](#) auf Seite 134

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 34
- [Synchronisation deaktivieren](#) auf Seite 36
- [Synchronisationsergebnisse anzeigen](#) auf Seite 35

Synchronisationen starten

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

Um regelmäßige Synchronisationen auszuführen

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

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

Um die initiale Synchronisation manuell zu starten

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

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

- Wenn eine weitere Synchronisation mit derselben Startkonfiguration gestartet wird, wird dieser Prozess gestoppt und erhält den Ausführungsstatus **Frozen**. Es wird eine Fehlermeldung in die Protokolldatei des One Identity Manager Service geschrieben.
 - Stellen Sie sicher, dass Startkonfigurationen, die in Startfolgen verwendet werden, nicht gleichzeitig einzeln gestartet werden. Weisen Sie den Startfolgen und Startkonfigurationen unterschiedliche Zeitpläne zu.
- Wenn eine weitere Synchronisation mit einer anderen Startkonfiguration gestartet

wird, die dasselbe Zielsystem anspricht, kann das zu Synchronisationsfehlern oder Datenverlust führen. Legen Sie an den Startkonfigurationen fest, wie sich der One Identity Manager in diesem Fall verhalten soll.

- Stellen Sie über den Zeitplan sicher, dass die Startkonfigurationen nacheinander ausgeführt werden.
- Gruppieren Sie die Startkonfigurationen mit gleichem Startverhalten.

Synchronisationsergebnisse anzeigen

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

Um das Protokoll einer Synchronisation anzuzeigen

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

In der Navigationsansicht werden die Protokolle aller abgeschlossenen Synchronisationsläufe angezeigt.

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

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

Um das Protokoll einer Provisionierung anzuzeigen

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

In der Navigationsansicht werden die Protokolle aller abgeschlossenen Provisionierungsprozesse angezeigt.

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

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

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

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

Verwandte Themen

- [Synchronisationsprotokoll konfigurieren](#) auf Seite 25
- [Fehleranalyse](#) auf Seite 40

Synchronisation deaktivieren

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

Um regelmäßige Synchronisationen zu verhindern

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

Synchronisationen können nun nur noch manuell gestartet werden.

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

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

Um das Synchronisationsprojekt zu deaktivieren

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

Einzelobjekte synchronisieren

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

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

Um ein Einzelobjekt zu synchronisieren

1. Wählen Sie im Manager die Kategorie **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.

Detaillierte Informationen zum Thema

- [Einzelobjektsynchronisation konfigurieren](#) auf Seite 31

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 37
- [Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen](#) auf Seite 39
- [Benutzerkonten über Kontendefinitionen verwalten](#) auf Seite 40

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

- a. Wählen Sie auf dem Formular für den Zielsystemabgleich das Objekt.
 - b. Öffnen Sie das Kontextmenü und klicken Sie **Objekt anzeigen**.
3. Wählen Sie die Objekte, die Sie nachbearbeiten möchten. Mehrfachauswahl ist möglich.
 4. Klicken Sie in der Formularelementeiste 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. Die Markierung Ausstehend wird für das Objekt entfernt. Indirekte Mitgliedschaften können nicht gelöscht werden.
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung Ausstehend wird für das Objekt entfernt. Die Methode löst das Ereignis <code>HandleOutstanding</code> aus. Dadurch wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt. Voraussetzungen: <ul style="list-style-type: none"> • Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen.

Symbol	Methode	Beschreibung
		<ul style="list-style-type: none"> 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 Formularymbolleiste .

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

- Wählen Sie im Manager die Kategorie **SharePoint Online | Basisdaten zur Konfiguration | Zielsystemtypen**.
- Wählen Sie in der Ergebnisliste den Zielsystemtyp **SharePoint Online**.
- Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.
- Weisen Sie im Bereich **Zuordnungen hinzufügen** die kundenspezifischen Tabellen zu, für die Sie ausstehende Objekte behandeln möchten.
- Speichern Sie die Änderungen.
- Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
- Wählen Sie die kundenspezifischen Tabellen, für die ausstehende Objekte in das

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

Verwandte Themen

- [Ausstehende Objekte nachbehandeln](#) auf Seite 37

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 67

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 35
- [Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen](#) auf Seite 26

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 angebotenen 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 angebotenen 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 43
- [Automatische Zuordnung von Personen zu SharePoint Online Benutzerkonten](#) auf Seite 62

Kontendefinitionen für SharePoint Online Benutzerkonten

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

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 44
- [Automatisierungsgrade bearbeiten](#) auf Seite 47
- [Abbildungsvorschriften für IT Betriebsdaten erstellen](#) auf Seite 50

- [IT Betriebsdaten erfassen](#) auf Seite 51
- [Zuweisen der Kontendefinition an Personen](#) auf Seite 54
- [Kontendefinitionen an Zielsysteme zuweisen](#) auf Seite 59

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.

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 von Kontendefinitionen](#) auf Seite 44
- [Kontendefinitionen erstellen](#) auf Seite 44

Stammdaten von 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	Vorausgesetzte Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch mitbestellt oder zugeordnet. TIPP: Sie können hier die Kontendefinition des zugehörigen Azure Active Directory Mandanten eintragen. In diesem Fall wird für die Person zunächst ein Azure Active Directory Benutzerkonto erzeugt. Ist dieses 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 an Personen. Erfassen Sie einen Wert zwischen 0 und 1. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter QER CalculateRiskIndex aktiviert ist. Ausführliche Informationen finden Sie im <i>One Identity Manager Administrationshandbuch für Risikobewertungen</i> .
Leistungsposition	Leistungsposition, über welche die Kontendefinition im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.
IT Shop	Angabe, ob die Kontendefinition über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Personen und Rollen außerhalb des IT Shop zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von den Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig.

Eigenschaft	Beschreibung
Automatische Zuweisung zu Personen	<p>Angabe, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Beim Speichern wird die Kontendefinition an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine Person neu angelegt wird, erhält sie ebenfalls automatisch diese Kontendefinition.</p> <p>WICHTIG: Aktivieren Sie diese Option nur, wenn sichergestellt ist, dass alle aktuell in der Datenbank vorhandenen internen Personen sowie alle zukünftig neu hinzuzufügenden internen Personen ein Benutzerkonto in diesem Zielsystem erhalten sollen!</p> <p>Um die automatische Zuweisung der Kontendefinition an alle Personen zu entfernen, deaktivieren Sie die Option. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.</p>
Kontendefinition bei dauerhafter Deaktivierung beibehalten	<p>Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Personen.</p> <p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>
Kontendefinition bei zeitweiliger Deaktivierung beibehalten	<p>Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Personen.</p> <p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>
Kontendefinition bei verzögertem Löschen beibehalten	<p>Angabe zur Zuweisung der Kontendefinition bei verzögertem Löschen von Personen.</p> <p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>
Kontendefinition bei Sicherheitsgefährdung beibehalten	<p>Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Personen.</p> <p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>

Eigenschaft	Beschreibung
Ressourcentyp	Ressourcentyp zur Gruppierung von.
Freies Feld 01- Freies Feld 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Automatisierungsgrade 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.

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 von Automatisierungsgraden](#) auf Seite 48
- [IT Betriebsdaten erfassen](#) auf Seite 51

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 von Kontendefinitionen](#) auf Seite 44
- [Kontendefinitionen bearbeiten](#) auf Seite 44

Stammdaten von Automatisierungsgraden

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	Angabe, ob Daten an Benutzerkonten, die sich aus den IT Betriebsdaten bilden, automatisch aktualisiert werden. Zulässige Werte sind: <ul style="list-style-type: none">• Niemals: Die Daten werden nicht aktualisiert.• Immer: Die Daten werden immer aktualisiert.• Nur initial: Die Daten werden nur initial ermittelt.
Gruppen bei zeitweiliger Deaktivierung	Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.

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

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 bzw. 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
- 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** und erfassen Sie folgende Informationen.

Tabelle 10: Abbildungsvorschrift für IT Betriebsdaten

Eigenschaft	Beschreibung
Spalte	Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript <code>TSB_ITDataFromOrg</code> verwenden.
Quelle	Angabe, welche Rolle verwendet wird, um die Eigenschaften für das Benutzerkonto zu ermitteln. Zur Auswahl stehen: <ul style="list-style-type: none">• Primäre Abteilung• Primärer Standort• Primäre Kostenstelle• Primäre Geschäftsrolle <p>HINWEIS: Verwenden Sie die primäre Geschäftsrolle nur, wenn das Geschäftsrollenmodul vorhanden ist.</p> <ul style="list-style-type: none">• keine Angabe Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option Immer Standardwert verwenden setzen.

Eigenschaft	Beschreibung
Standardwert	Standardwert der Eigenschaft für das Benutzerkonto einer Person, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann.
Immer Standardwert verwenden	Angabe, ob die Eigenschaft des Benutzerkontos immer mit dem Standardwert besetzt wird. Es erfolgt keine dynamische Ermittlung der IT Betriebsdaten aus einer Rolle.
Benachrichtigung bei Verwendung des Standards	Angabe, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage Person - Erstellung neues Benutzerkontos mit Standardwerten verwendet. Um die Mailvorlage zu ändern, passen Sie den Konfigurationsparameter TargetSystem SharePointOnline Accounts MailTemplateDefaultValues an.

4. Speichern Sie die Änderungen.

IT Betriebsdaten erfassen

Um für eine Person Benutzerkonten mit dem Automatisierungsgrad **Full managed** zu erzeugen, müssen die benötigten IT Betriebsdaten ermittelt werden. Welche IT Betriebsdaten für welches Zielsystem konkret verwendet werden sollen, wird an den Geschäftsrollen, Abteilungen, Kostenstellen oder Standorten definiert. Einer Person wird eine 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 A und eine Kontendefinition B für die administrativen Benutzerkonten des Mandanten A. In der


Abbildungsvorschrift der IT Betriebsdaten für die Kontendefinitionen A und B legen Sie die Eigenschaft "Abteilung" zur Ermittlung der gültigen IT Betriebsdaten fest.

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

Um IT Betriebsdaten festzulegen

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

Tabelle 11: IT Betriebsdaten

Eigenschaft	Beschreibung
Wirksam für	<p>Anwendungsbereich der IT Betriebsdaten. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden.</p> <p>Um den Anwendungsbereich festzulegen</p> <ol style="list-style-type: none">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	<p>Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird.</p> <p>In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript TSB_ITDataFromOrg verwenden.</p>
Wert	<p>Konkreter Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.</p>

4. Speichern Sie die Änderungen.

Verwandte Themen

- [Abbildungsvorschriften für IT Betriebsdaten erstellen](#) auf Seite 50

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, 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.

Alter Wert: Aktueller Wert der Objekteigenschaft.

Neuer Wert: Wert, den die Objekteigenschaft durch die Änderung an den IT Betriebsdaten annehmen würde.

Auswahl: Angabe, ob die Änderung für das Benutzerkonto übernommen werden soll.

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

Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinition an Personen

Kontendefinitionen werden an die Personen des Unternehmens zugewiesen.

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

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

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

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

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

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

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

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

Detaillierte Informationen zum Thema

- [Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 55
- [Kontendefinitionen an Geschäftsrollen zuweisen](#) auf Seite 55
- [Kontendefinitionen an alle Personen zuweisen](#) auf Seite 56
- [Kontendefinitionen direkt an Personen zuweisen](#) auf Seite 56

- [Kontendefinitionen an Systemrollen zuweisen](#) auf Seite 57
- [Kontendefinitionen in den IT Shop aufnehmen](#) auf Seite 57


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

Installierte Module: Geschäftsrollenmodul

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. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Geschäftsrolle und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Kontendefinitionen an alle Personen zuweisen

Um eine Kontendefinition an alle Personen zuzuweisen

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

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

5. Speichern Sie die Änderungen.

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

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


Kontendefinitionen direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **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

Installierte Module: Systemrollenmodul


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

Um Kontendefinitionen in eine Systemrolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **SharePoint 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

1. Wählen Sie im Manager die Kategorie **SharePoint Online | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).
- ODER -
Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontendefinition an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen

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

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **SharePoint Online | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**(bei nicht-rollenbasierter Anmeldung).
- ODER -
Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen**(bei rollenbasierter Anmeldung).
 2. Wählen Sie in der Ergebnisliste die Kontendefinition.
 3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
 4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
 5. Klicken Sie **OK**.
- Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.

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

Verwandte Themen

- [Stammdaten von Kontendefinitionen](#) auf Seite 44

Kontendefinitionen an Zielsysteme zuweisen

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

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

Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand **Linked**). 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 Websitesammlung.
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 62
- [Stammdaten von Automatisierungsgraden](#) auf Seite 48

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. Deaktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.
 - e. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Personen.
 - a. Wählen Sie im Manager die Kategorie **SharePoint 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**.
Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
 - d. 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 Anwenderhandbuch für das Web Portal*.

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

- a. Wählen Sie im Manager die Kategorie **SharePoint Online | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**(bei nicht-rollenbasierter Anmeldung).
 - ODER -
 - Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen**(bei rollenbasierter Anmeldung).
- b. Wählen Sie in der Ergebnisliste die Kontendefinition.
- c. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
- d. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
- e. Klicken Sie **OK**.

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

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. Für die automatische Personenzuordnung definieren Sie Kriterien für die Ermittlung der Personen. Wird durch den eingesetzten Modus ein Benutzerkonto mit einer Person verbunden, so erhält das Benutzerkonto durch interne Verarbeitung den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Abhängig davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden.

Schalten Sie das Verfahren im laufenden Betrieb ein, erfolgt ab diesem Zeitpunkt die automatische Zuordnung der Personen zu Benutzerkonten. Deaktivieren Sie das Verfahren zu einem späteren Zeitpunkt wieder, wirkt sich diese Änderung nur auf Benutzerkonten aus, die ab diesem Zeitpunkt angelegt oder aktualisiert werden. Bereits vorhandene Zuordnungen von Personen zu Benutzerkonten bleiben bestehen.

HINWEIS: Für administrative Benutzerkonten wird empfohlen, die Zuordnung der Personen nicht über die automatische Personenzuordnung vorzunehmen. Ordnen Sie Personen zu administrativen Benutzerkonten über die Aufgabe **Stammdaten bearbeiten** am jeweiligen Benutzerkonto zu.

Voraussetzungen:

- 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 40.

Verwandte Themen

- [Kontendefinitionen erstellen](#) auf Seite 44
- [Kontendefinitionen an Zielsysteme zuweisen](#) auf Seite 59
- [Automatisierungsgrad an SharePoint Online Benutzerkonten ändern](#) auf Seite 66
- [Suchkriterien für die automatische Personenzuordnung bearbeiten](#) auf Seite 63

Suchkriterien für die automatische Personenzuordnung bearbeiten

Die Kriterien für die Personenzuordnung werden an der Websitesammlung definiert. Dabei legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person dem Benutzerkonto zugeordnet werden kann. Die Suchkriterien können Sie durch Formatdefinitionen weiter einschränken. Das

zusammengestellte Suchkriterium wird in XML-Notation in die Spalte **Suchkriterien für die automatische Personenzuordnung** (AccountToPersonMatchingRule) der Tabelle 03SSite geschrieben.

Suchkriterien werden bei der automatischen Zuordnung von Personen zu Benutzerkonten ausgewertet. Darüber hinaus können Sie anhand der Suchkriterien eine Vorschlagsliste für die Personenzuordnung an Benutzerkonten erzeugen und die Zuordnung direkt ausführen.

HINWEIS: Bei der Zuordnung der Personen zu Benutzerkonten anhand der Suchkriterien erhalten die Benutzerkonten den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Abhängig davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden.

Für administrative Benutzerkonten wird empfohlen, die Zuordnung nicht anhand der Suchkriterien vorzunehmen. Ordnen Sie Personen zu administrativen Benutzerkonten über die Aufgabe **Stammdaten bearbeiten** am jeweiligen Benutzerkonto zu.

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 12: 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 62
- [Personen suchen und direkt an Benutzerkonten zuordnen](#) auf Seite 65

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 13: 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.

Automatisierungsgrad an 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.

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 und den Automatisierungsgrad zu.
 - 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**.

Detaillierte Informationen zum Thema

- [Kontendefinitionen an Zielsysteme zuweisen](#) auf Seite 59

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 68
- [Unterstützte Typen von Benutzerkonten](#) auf Seite 70

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 14: Identitäten von Benutzerkonten

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

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

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

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

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

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

- Privilegiertes Benutzerkonto

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

Detaillierte Informationen zum Thema

- [Standardbenutzerkonten](#) auf Seite 71
- [Administrative Benutzerkonten](#) auf Seite 72
- [Privilegierte Benutzerkonten](#) auf Seite 75

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

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

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

Verwandte Themen

- [Kontendefinitionen für SharePoint Online Benutzerkonten](#) auf Seite 43

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 73
- [Administrative Benutzerkonten für mehrere Personen bereitstellen](#) auf Seite 74

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 74
- 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 Dummy-Person vorhanden sein. Die Dummy-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 Dummy-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 Dummy-Person.

TIPP: Als Zielsystemverantwortlicher können Sie über die Schaltfläche  eine neue Dummy-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 73
- 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, dass privilegierte Benutzerkonten die Berechtigungen des Standardbenutzers erben, definieren Sie eine Abbildungsvorschrift für die Spalte `IsGroupAccount` mit dem Standardwert **0** und aktivieren Sie die Option **Immer Standardwert verwenden**.
5. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem.
Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.
 6. Weisen Sie die Kontendefinition direkt an die Personen zu, die mit privilegierten Benutzerkonten arbeiten sollen.
Durch die Zuweisung der Kontendefinition an eine Person wird über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

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

Verwandte Themen

- [Kontendefinitionen für SharePoint Online Benutzerkonten](#) auf Seite 43

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 können die Benutzer verschiedene Berechtigungen haben, die folgendermaßen im One Identity Manager abgebildet werden:

- Berechtigung zur Nutzung von SharePoint Online Gruppen (Tabelle 03SGroup)
- Berechtigung zur Nutzung von SharePoint Online Rollen (Tabelle 03SRLAsgn)

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 03SUserInGroup)
 - Zuweisungen von Rollen an Benutzerkonten (Tabelle 03SUserHasRLAsgn)

Zuweisen von SharePoint Online Berechtigungen an SharePoint Online Benutzerkonten im One Identity Manager

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 in einer Systemrolle Systemberechtigungen aus unterschiedlichen Zielsystemen zusammengefasst werden.

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

Voraussetzungen

- Für Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen ist die Zuweisung von Personen, SharePoint Online Rollen und SharePoint Online Gruppen erlaubt.

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.

- An den Benutzerkonten ist die Option **Gruppenauthentifiziert** deaktiviert.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.
- Benutzerkonten und SharePoint Online Berechtigungen gehören zur selben Websitesammlung.

Ausführliche Informationen finden Sie in den folgenden Handbüchern.

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

Detaillierte Informationen zum Thema

- [SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 80
- [SharePoint Online Berechtigungen an Geschäftsrollen zuweisen](#) auf Seite 82
- [SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen](#) auf Seite 86
- [SharePoint Online Berechtigungen in Systemrollen aufnehmen](#) auf Seite 83
- [SharePoint Online Berechtigungen in den IT Shop aufnehmen](#) auf Seite 84
- [SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen](#) auf Seite 87
- [SharePoint Online Rollen an SharePoint Online Gruppen zuweisen](#) auf Seite 87

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

Verwandte Themen

- [SharePoint Online Berechtigungen an Geschäftsrollen zuweisen](#) auf Seite 82
- [SharePoint Online Berechtigungen in Systemrollen aufnehmen](#) auf Seite 83
- [SharePoint Online Berechtigungen in den IT Shop aufnehmen](#) auf Seite 84
- [SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen](#) auf Seite 86
- [SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen](#) auf Seite 87
- [One Identity Manager Benutzer für die Verwaltung einer SharePoint Online-Umgebung](#) auf Seite 9

SharePoint Online Berechtigungen an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul


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

Um eine Berechtigung an Geschäftsrollen zuzuweisen (bei nicht-rollebasierter 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. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

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

Um eine Zuweisung zu entfernen

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

Um Berechtigungen an eine Geschäftsrolle zuzuweisen (bei rollebasierter 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.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Berechtigungen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 80

- [SharePoint Online Berechtigungen in Systemrollen aufnehmen](#) auf Seite 83
- [SharePoint Online Berechtigungen in den IT Shop aufnehmen](#) auf Seite 84
- [SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen](#) auf Seite 86
- [SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen](#) auf Seite 87
- [One Identity Manager Benutzer für die Verwaltung einer SharePoint Online-Umgebung](#) auf Seite 9

SharePoint Online Berechtigungen in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

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


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

Um eine Berechtigung an Systemrollen zuzuweisen

1. Wählen Sie 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

- [SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 80
- [SharePoint Online Berechtigungen an Geschäftsrollen zuweisen](#) auf Seite 82
- [SharePoint Online Berechtigungen in den IT Shop aufnehmen](#) auf Seite 84

- [SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen](#) auf Seite 86
- [SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen](#) auf Seite 87

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

Um eine Berechtigung aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager 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. Entfernen Sie im Bereich **Zuordnungen entfernen** die Berechtigung aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Berechtigung aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager 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 112](#)
- [Allgemeine Stammdaten für SharePoint Online Rollen auf Seite 127](#)
- [SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 80](#)
- [SharePoint Online Berechtigungen an Geschäftsrollen zuweisen auf Seite 82](#)
- [SharePoint Online Berechtigungen in Systemrollen aufnehmen auf Seite 83](#)
- [SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 86](#)
- [SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 87](#)
- [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 Gruppe.
 - ODER -
 - Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.
 - ODER -
 - Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 87](#)
- [SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 80](#)
- [SharePoint Online Berechtigungen an Geschäftsrollen zuweisen auf Seite 82](#)

- [SharePoint Online Berechtigungen in Systemrollen aufnehmen](#) auf Seite 83
- [SharePoint Online Berechtigungen in den IT Shop aufnehmen](#) auf Seite 84

SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen

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

Um Berechtigungen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie 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.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Berechtigungen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen](#) auf Seite 86
- [SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 80
- [SharePoint Online Berechtigungen an Geschäftsrollen zuweisen](#) auf Seite 82
- [SharePoint Online Berechtigungen in Systemrollen aufnehmen](#) auf Seite 83
- [SharePoint Online Berechtigungen in den IT Shop aufnehmen](#) auf Seite 84

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

Verwandte Themen

- [Allgemeine Stammdaten für SharePoint Online Berechtigungsstufen](#) auf Seite 117
- [SharePoint Online Gruppen an SharePoint Online Rollen zuweisen](#) auf Seite 88
- [SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 80
- [SharePoint Online Berechtigungen an Geschäftsrollen zuweisen](#) auf Seite 82
- [SharePoint Online Berechtigungen in Systemrollen aufnehmen](#) auf Seite 83
- [SharePoint Online Berechtigungen in den IT Shop aufnehmen](#) auf Seite 84
- [SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen](#) auf Seite 86
- [SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen](#) auf Seite 87

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

- [Allgemeine Stammdaten für SharePoint Online Berechtigungsstufen](#) auf Seite 117
- [SharePoint Online Rollen an SharePoint Online Gruppen zuweisen](#) auf Seite 87
- [SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 80
- [SharePoint Online Berechtigungen an Geschäftsrollen zuweisen](#) auf Seite 82
- [SharePoint Online Berechtigungen in den IT Shop aufnehmen](#) auf Seite 84
- [SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen](#) auf Seite 86
- [SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen](#) auf Seite 87

Wirksamkeit von SharePoint Online Berechtigungszuweisungen

Tabelle 15: Konfigurationsparameter für die bedingte Vererbung

Konfigurationsparameter	Wirkung bei Aktivierung
QER Structures Inherit GroupExclusion	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Wirksamkeit von Gruppenmitgliedschaften. Ist der Parameter aktiviert, können aufgrund von Ausschlussdefinitionen die Gruppenmitgliedschaften reduziert werden. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.

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

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

HINWEIS:

- Ein wechselseitiger Ausschluss zweier Gruppen kann nicht definiert werden. Das heißt, die Festlegung "Gruppe A schließt Gruppe B aus" UND "Gruppe B schließt

Gruppe A aus" ist nicht zulässig.

- Für eine Gruppe muss jede auszuschließende Gruppe einzeln bekannt gegeben werden. Ausschlussdefinitionen werden nicht vererbt.

Die Wirksamkeit der Zuweisungen wird in den Tabellen 03SUserIn03SGroup und 03SBaseTreeHasGroup über die Spalte XIsInEffect abgebildet.

Beispiel für die 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 16: Festlegen der ausgeschlossenen Gruppen (Tabelle 03SGroupExclusion)

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

Tabelle 17: 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 18: 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 | Inherit | GroupExclusion** ist aktiviert.
- 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 31**.

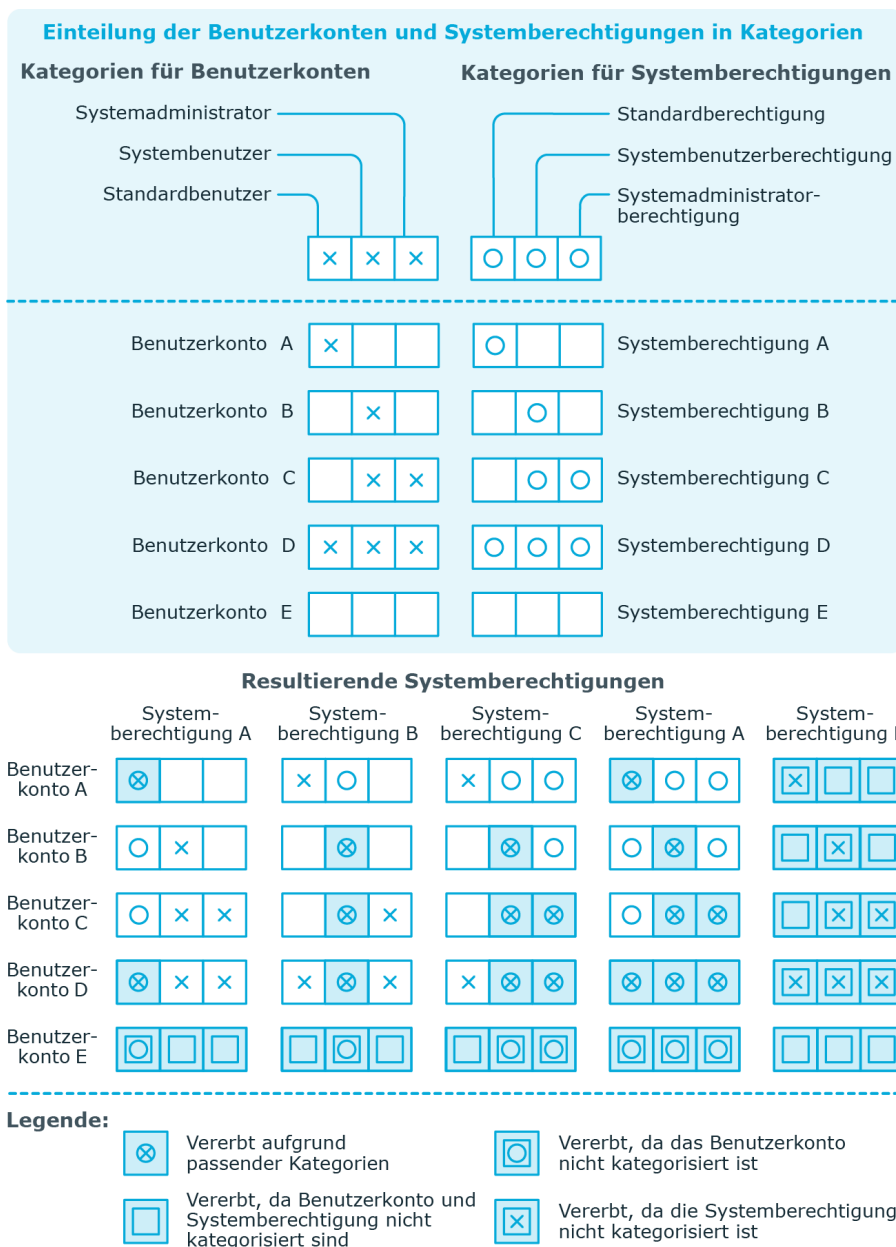
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto vererbt. Ist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

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

Tabelle 19: 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

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

Verwandte Themen

- [Festlegen der Kategorien für die Vererbung von SharePoint Online Gruppen auf Seite 120](#)
- [Stammdaten eines gruppenauthentifizierten Benutzerkontos auf Seite 105](#)
- [Stammdaten eines benutzerauthentifizierten Benutzerkontos auf Seite 102](#)
- [Stammdaten für SharePoint Online Gruppen auf Seite 112](#)


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 Berichtes 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 20: 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](#) auf Seite 96
- [SharePoint Online Gruppen](#) auf Seite 110
- [SharePoint Online Benutzerkonten](#) auf Seite 100
- [SharePoint Online Berechtigungsstufen](#) auf Seite 115
- [SharePoint Online Websitesammlungen](#) auf Seite 118
- [SharePoint Online Websites](#) auf Seite 122
- [SharePoint Online Rollen](#) auf Seite 126

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

- [Allgemeine Stammdaten für SharePoint Online Mandanten](#) auf Seite 97
- [Synchronisieren einer SharePoint Online-Umgebung](#) auf Seite 12
- [Verarbeitung von Systemobjekten](#) auf Seite 145

Allgemeine Stammdaten für SharePoint Online Mandanten

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

Tabelle 21: 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.
Zielsystemverantwortliche	<p>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.</p> <p>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.</p>
Synchronisiert durch	<p>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.</p> <p>Beim Erstellen eines Mandanten mit dem Synchronisation Editor wird One Identity Manager verwendet.</p>

Eigenschaft	Beschreibung									
	<p>Tabelle 22: Zulässige Werte</p> <table border="1"> <thead> <tr> <th>Wert</th> <th>Synchronisation durch</th> <th>Provisionierung durch</th> </tr> </thead> <tbody> <tr> <td>One Identity Manager</td> <td>SharePoint Online Konnektor</td> <td>SharePoint Online Konnektor</td> </tr> <tr> <td>Keine Synchronisation</td> <td>keine</td> <td>keine</td> </tr> </tbody> </table> <p>HINWEIS: Wenn Sie Keine Synchronisation festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.</p>	Wert	Synchronisation durch	Provisionierung durch	One Identity Manager	SharePoint Online Konnektor	SharePoint Online Konnektor	Keine Synchronisation	keine	keine
Wert	Synchronisation durch	Provisionierung durch								
One Identity Manager	SharePoint Online Konnektor	SharePoint Online Konnektor								
Keine Synchronisation	keine	keine								
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.									
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 139

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 einen SharePoint Online Mandanten auf Seite 99
Suchkriterien für die Personenzuordnung definieren	Suchkriterien für die automatische Personenzuordnung bearbeiten auf Seite 63
Synchronisationsprojekt bearbeiten	Synchronisationsprojekt für einen SharePoint Online Mandanten bearbeiten auf Seite 99
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 36

Überblick über einen 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 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 Synchronisation 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 Synchronisation 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. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten....**

Verwandte Themen

- [Anpassen einer Synchronisationskonfiguration](#) auf Seite 26

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 68
- [Managen von SharePoint Online Benutzerkonten und Personen](#) auf Seite 42
- [Kontendefinitionen für SharePoint Online Benutzerkonten](#) auf Seite 43
- [Standardprojektvorlage für SharePoint Online](#) auf Seite 144
- [Stammdaten für SharePoint Online Benutzerkonten bearbeiten](#) auf Seite 101
- [SharePoint Online Benutzerkonten löschen und wiederherstellen](#) auf Seite 109
- [Managen von Zuweisungen von SharePoint Online Gruppen und Rollen](#) auf Seite 78

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.

Detaillierte Informationen zum Thema

- [SharePoint Online Benutzerkonten](#) auf Seite 100
- [Erfassen der Stammdaten für SharePoint Online Benutzerkonten](#) auf Seite 102

Verwandte Themen

- [Stammdaten für SharePoint Online Benutzerkonten bearbeiten](#) auf Seite 101
- [SharePoint Online Benutzerkonten löschen und wiederherstellen](#) auf Seite 109

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 und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- [Erfassen der Stammdaten für SharePoint Online Benutzerkonten](#) auf Seite 102

Verwandte Themen

- [SharePoint Online Benutzerkonten erstellen](#) auf Seite 101
- [SharePoint Online Benutzerkonten löschen und wiederherstellen](#) auf Seite 109

Erfassen der Stammdaten für SharePoint Online Benutzerkonten

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


Detaillierte Informationen zum Thema

- [Stammdaten eines gruppenauthentifizierten Benutzerkontos](#) auf Seite 105
- [Stammdaten eines benutzerauthentifizierten Benutzerkontos](#) auf Seite 102

Stammdaten eines benutzerauthentifizierten Benutzerkontos

Für ein benutzerauthentifiziertes Benutzerkonto erfassen Sie die folgenden Stammdaten.

Tabelle 23: Stammdaten eines benutzerauthentifizierten Benutzerkontos

Eigenschaft	Beschreibung
Person	<p>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.</p> <p>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</p>

Eigenschaft	Beschreibung
Kontendefinition	<p>gewählten Identitätstyp.</p> <p>Kontendefinition, über die das Benutzerkonto erstellt wurde.</p> <p>Die Kontendefinition wird benutzt, um die Stammdaten des Benutzerkontos automatisch zu befüllen und um einen Automatisierungsgrad für das Benutzerkonto festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Person und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein.</p> <p>HINWEIS: Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden.</p> <p>HINWEIS: Sollen Personen ihre SharePoint Online Benutzerkonten über Kontendefinitionen erhalten, müssen die Personen Benutzerkonten im dazugehörigen Azure Active Directory Mandanten besitzen, der am SharePoint Online Mandanten hinterlegt ist.</p>
Automatisierungsgrad	<p>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.</p>
Websitesammlung	<p>Websitesammlung, in der das Benutzerkonto genutzt wird.</p>
Prinzipal-Typ	<p>Art des Prinzipals (Benutzer, Domänengruppe).</p>
Authentifizierungsmodus	<p>Authentifizierungsmodus, der bei der Anmeldung mit diesem Benutzerkonto am SharePoint Online Server genutzt wird. Für SharePoint Online gilt AzureAD als einziger Authentifizierungsmodus.</p>
Authentifizierungsobjekt	<p>Authentifizierungsobjekt, welches das Benutzerkonto referenziert.</p> <p>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.</p> <p>Einem benutzerauthentifizierten Benutzerkonto können folgende Authentifizierungsobjekte zugeordnet werden:</p> <ul style="list-style-type: none"> • Azure Active Directory Benutzerkonten aus dem Mandanten, der dem SharePoint Online Mandanten zugeordnet ist

Eigenschaft	Beschreibung
Titel	<p>HINWEIS: Das SharePoint Online Benutzerkonto wird auch dann erstellt, wenn das Benutzerkonto, das als Authentifizierungsobjekt genutzt wird, deaktiviert oder gesperrt ist.</p> <p>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.</p>
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 <i>One Identity Manager Administrationshandbuch für Risikobewertungen</i> .
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	<p>Typ der Identität des Benutzerkontos. Zulässige Werte sind:</p> <ul style="list-style-type: none"> • Primäre Identität: Standardbenutzerkonto einer Person. • Organisatorische Identität: Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen. • Persönliche Administratoridentität: Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird. • Zusatzidentität: Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird. • Gruppenidentität: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen

Eigenschaft	Beschreibung
	genutzt wird. Weisen Sie alle Personen zu, die das Benutzerkonto nutzen. <ul style="list-style-type: none"> • Dienstidentität: Dienstkonto.
Privilegiertes Benutzerkonto	Angabe, ob es sich um ein privilegiertes Benutzerkonto handelt.
Gruppen erbbar	Angabe, ob das Benutzerkonto SharePoint Online Rollen und Gruppen über die Person erben darf. Ist die Option aktiviert, werden SharePoint Online Rollen und Gruppen über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt. <ul style="list-style-type: none"> • Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Person eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Gruppe nur, wenn die Option aktiviert ist.
Administrator	Angabe, ob das Benutzerkonto Administrator einer Websitesammlung ist.
Versteckt	Angabe, ob das Benutzerkonto in der Benutzeroberfläche angezeigt wird.


Detaillierte Informationen zum Thema

- [Kontendefinitionen für SharePoint Online Benutzerkonten](#) auf Seite 43
- [Festlegen der Kategorien für die Vererbung von SharePoint Online Gruppen](#) auf Seite 120
- [Automatische Zuordnung von Personen zu SharePoint Online Benutzerkonten](#) auf Seite 62
- [Unterstützte Typen von Benutzerkonten](#) auf Seite 70

Stammdaten eines gruppenthauthentifizierten Benutzerkontos

Für ein gruppenthauthentifiziertes Benutzerkonto erfassen Sie die folgenden Stammdaten.

Tabelle 24: Stammdaten eines gruppenauthentifizierten Benutzerkontos

Eigenschaft	Beschreibung
Person	<p>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.</p> <p>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.</p>
Websitesammlung	Websitesammlung, in der das Benutzerkonto genutzt wird.
Gruppenauthentifiziert	Angabe, ob das Authentifizierungsobjekt des Benutzerkontos eine Gruppe ist.
Authentifizierungsmodus	Authentifizierungsmodus, der bei der Anmeldung mit diesem Benutzerkonto am SharePoint Online Server genutzt wird. Für SharePoint Online gilt AzureAD als einziger Authentifizierungsmodus.
Authentifizierungsobjekt	<p>Authentifizierungsobjekt, welches das Benutzerkonto referenziert.</p> <p>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.</p> <p>Einem gruppenauthentifizierten Benutzerkonto können folgende Authentifizierungsobjekte zugeordnet werden:</p> <ul style="list-style-type: none"> • 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 wird standardmäßig aus dem Anzeigenamen des Authentifizierungsobjektes gebildet. Wenn kein Authentifizierungsobjekt zugeordnet ist, tragen Sie den

Eigenschaft	Beschreibung
	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 <i>One Identity Manager Administrationshandbuch für Risikobewertungen</i> .
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.
Identität	Typ der Identität des Benutzerkontos. Zulässige Werte sind: <ul style="list-style-type: none"> • Primäre Identität: Standardbenutzerkonto einer Person. • Organisatorische Identität: Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen. • Persönliche Administratoridentität: Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird. • Zusatzidentität: Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird. • Gruppenidentität: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird. Weisen Sie alle Personen zu, die das Benutzerkonto nutzen. • Dienstidentität: Dienstkonto.
Privilegiertes Benutzerkonto	Angabe, ob es sich um ein privilegiertes Benutzerkonto handelt.

Eigenschaft	Beschreibung
Administrator	Angabe, ob das Benutzerkonto Administrator einer Websitesammlung ist.
Versteckt	Angabe, ob das Benutzerkonto in der Benutzeroberfläche angezeigt wird.

Detaillierte Informationen zum Thema

- [Festlegen der Kategorien für die Vererbung von SharePoint Online Gruppen](#) auf Seite 120
- [Unterstützte Typen von Benutzerkonten](#) auf Seite 70

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 ein SharePoint Online Benutzerkonto auf Seite 108
Zusatzeigenschaften zuweisen	Zusatzeigenschaften zuweisen auf Seite 109
Gruppen zuweisen	SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 87
SharePoint Online Rollen zuweisen	SharePoint Online Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 87
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 36

Überblick über ein SharePoint Online Benutzerkonto

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 zuweisen


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

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

1. Wählen Sie 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.

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


SharePoint Online Benutzerkonten löschen und wiederherstellen

Wird ein Benutzerkonto im One Identity Manager gelöscht, wird es zunächst zum Löschen markiert. Das Benutzerkonto wird daraufhin gesperrt. Je nach Einstellung der Löschverzögerung wird das Benutzerkonto sofort oder zu einem späteren Zeitpunkt aus der One Identity Manager-Datenbank gelöscht.


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

gelöscht.

Um ein Benutzerkonto zu löschen, 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 , um das Benutzerkonto zu löschen.
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 .

Konfigurieren der Löschverzögerung

Standardmäßig werden Benutzerkonten mit einer Löschverzögerung von 30 Tagen endgültig aus der Datenbank entfernt. Bis zum Ablauf der Löschverzögerung besteht die Möglichkeit die Benutzerkonten wieder zu aktivieren. Nach Ablauf der Löschverzögerung werden die Benutzerkonten aus der Datenbank gelöscht und ein Wiederherstellen ist nicht mehr möglich. Eine abweichende Löschverzögerung konfigurieren Sie im Designer an der Tabelle O3SUser.

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.

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

Detaillierte Informationen zum Thema


- [Stammdaten für SharePoint Online Gruppen](#) auf Seite 112
- [Festlegen der Kategorien für die Vererbung von SharePoint Online Gruppen](#) auf Seite 120
- [Vererbung von SharePoint Online Gruppen anhand von Kategorien](#) auf Seite 91

Verwandte Themen

- [SharePoint Online Gruppen erstellen](#) auf Seite 111
- [SharePoint Online Gruppen löschen](#) auf Seite 115

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.

Detaillierte Informationen zum Thema

- [Stammdaten für SharePoint Online Gruppen](#) auf Seite 112
- [Zusätzliche Aufgaben zur Verwaltung von SharePoint Online Gruppen](#) auf Seite 114

Verwandte Themen

- [Stammdaten für SharePoint Online Gruppen bearbeiten](#) auf Seite 112
- [SharePoint Online Gruppen löschen](#) auf Seite 115

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.

Detaillierte Informationen zum Thema

- [Stammdaten für SharePoint Online Gruppen](#) auf Seite 112
- [Zusätzliche Aufgaben zur Verwaltung von SharePoint Online Gruppen](#) auf Seite 114

Verwandte Themen

- [SharePoint Online Gruppen erstellen](#) auf Seite 111
- [SharePoint Online Gruppen löschen](#) auf Seite 115

Stammdaten für SharePoint Online Gruppen

Für eine Gruppe erfassen Sie die folgenden Stammdaten.

Tabelle 25: 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	Angabe einer Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter QER CalculateRiskIndex aktiviert ist.

Eigenschaft	Beschreibung
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	Gibt an, 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	Angabe, ob die Gruppe über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.

Detaillierte Informationen zum Thema

- [Festlegen der Kategorien für die Vererbung von SharePoint Online Gruppen](#) auf Seite 120
- [Vererbung von SharePoint Online Gruppen anhand von Kategorien](#) auf Seite 91

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 114
Benutzerkonten zuweisen	SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 86
SharePoint Online Rollen zuweisen	SharePoint Online Rollen an SharePoint Online Gruppen zuweisen auf Seite 87
Systemrollen zuweisen	SharePoint Online Berechtigungen in Systemrollen aufnehmen auf Seite 83
Geschäftsrollen zuweisen	SharePoint Online Berechtigungen an Geschäftsrollen zuweisen auf Seite 82
Organisationen zuweisen	SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 80
Gruppen ausschließen	Wirksamkeit von SharePoint Online Berechtigungszuweisungen auf Seite 89
In IT Shop aufnehmen	SharePoint Online Berechtigungen in den IT Shop aufnehmen auf Seite 84
Zusatzeigenschaften zuweisen	Zusatzeigenschaften an SharePoint Online Gruppen zuweisen auf Seite 115
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 36

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.

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.

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

SharePoint Online Gruppen löschen

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

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

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 116
- [Stammdaten für SharePoint Online Berechtigungsstufen bearbeiten](#) auf Seite 116
- [Allgemeine Stammdaten für SharePoint Online Berechtigungsstufen](#) auf Seite 117
- [Löschen von SharePoint Online Berechtigungsstufen](#) auf Seite 117
- [Einzelobjekte synchronisieren](#) auf Seite 36

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 bearbeiten](#) auf Seite 116
- [Löschen von SharePoint Online Berechtigungsstufen](#) auf Seite 117

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

- [Allgemeine Stammdaten für SharePoint Online Berechtigungsstufen](#) auf Seite 117
- [SharePoint Online Berechtigungsstufen erstellen](#) auf Seite 116

Allgemeine Stammdaten für SharePoint Online Berechtigungsstufen

Für eine Berechtigungsstufe erfassen Sie die folgenden Stammdaten.

Tabelle 26: 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.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Versteckt	Angabe, ob eine SharePoint Online Rolle mit dieser Berechtigungsstufe an Benutzerkonten oder Gruppen zugewiesen werden kann.

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**.

Löschen von SharePoint Online Berechtigungsstufen

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 Löscherzögerung konfiguriert ist, wird die Berechtigungsstufe zum Löschen markiert und erst nach Ablauf der Löscherzögerung endgültig gelöscht. Während dieser Zeit kann die Berechtigungsstufe wiederhergestellt werden. Berechtigungsstufen mit einer Löscherzögerung 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. Ihre Eigenschaften können im One Identity Manager nicht bearbeitet werden. Die innerhalb einer Websitesammlung verwalteten Zugriffsrechte können im One Identity Manager bearbeitet werden. Dafür werden SharePoint Online Rollen, Gruppen und Benutzerkonten in die One Identity Manager-Datenbank eingelesen.

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

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.

Detaillierte Informationen zum Thema

- [Allgemeine Stammdaten einer SharePoint Online Websitesammlung](#) auf Seite 119
- [Festlegen der Kategorien für die Vererbung von SharePoint Online Gruppen](#) auf Seite 120

Allgemeine Stammdaten einer SharePoint Online Websitesammlung

Für Websitesammlungen werden die folgende Stammdaten abgebildet.

| **HINWEIS:** Lediglich die Kontendefinition der Websitesammlung kann bearbeitet werden.

Tabelle 27: 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.
Letzte inhaltsrelevante Änderung	Zeitpunkt der letzten inhaltsrelevanten Änderung, die an einem Objekt dieser Websitesammlung vorgenommen wurde.

Verwandte Themen

- [Kontendefinitionen für SharePoint Online Benutzerkonten](#) auf Seite 43

Adressdaten einer SharePoint Online Websitesammlung

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

Tabelle 28: 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.

Festlegen der Kategorien für die Vererbung von SharePoint Online Gruppen

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

Um Kategorien zu definieren

1. Wählen Sie im Manager in der Kategorie **SharePoint Online | Websitesammlungen** die Websitesammlung.
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 91

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 eine SharePoint Online Websitesammlung auf Seite 121
Suchkriterien für die Personenzuordnung definieren	Suchkriterien für die automatische Personenzuordnung bearbeiten auf Seite 63
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 36

Überblick über eine SharePoint Online Websitesammlung

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.

Um die Eigenschaften einer Website zu bearbeiten

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

Detaillierte Informationen zum Thema

- [Allgemeine Stammdaten von SharePoint Online Websites](#) auf Seite 122
- [Adressdaten von SharePoint Online Websites](#) auf Seite 123
- [Designinformationen von SharePoint Online Websites](#) auf Seite 124
- [Einzelobjekte synchronisieren](#) auf Seite 36

Allgemeine Stammdaten von SharePoint Online Websites

Für Websites werden die folgenden allgemeine Stammdaten abgebildet.

Tabelle 29: 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.

Eigenschaft	Beschreibung
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.
Eigentümergeuppe	Die zugehörigen Eigentümergruppen der Website.
Besucherguppe	Die zugehörige Besuchergruppe der Website.
Autor	Verweis auf das Benutzerkonto, mit dem die Website erstellt wurde.
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 78](#)

Adressdaten von SharePoint Online Websites

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

Tabelle 30: Adressdaten einer Website

Eigenschaften	Beschreibung
URL relativ zum Server	URL der Website, relativ zur URL des Servers.
URL	Absolute URL der Website.
URL der Masterseite	URL der Masterseite, die für die Website genutzt wird.
Alternative Master URL	URL zu einer alternativen Masterseite, auf die sich die Website bezieht.

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 124

Designinformationen von SharePoint Online Websites

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

Tabelle 31: 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 123

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

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 122
- [Managen von Zuweisungen von SharePoint Online Gruppen und Rollen](#) auf Seite 78

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 115

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 127
- [Allgemeine Stammdaten für SharePoint Online Berechtigungsstufen](#) auf Seite 117

Allgemeine Stammdaten für SharePoint Online Rollen

Für SharePoint Online Rollen werden die folgenden Stammdaten abgebildet.

Tabelle 32: Allgemeine Stammdaten einer SharePoint Online Rolle

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

- [Allgemeine Stammdaten für SharePoint Online Berechtigungsstufen](#) auf Seite 117

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 eine SharePoint Online Rolle auf Seite 128
Benutzerkonten zuweisen	SharePoint Online Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 86
Gruppen zuweisen	SharePoint Online Gruppen an SharePoint Online Rollen zuweisen auf Seite 88
Systemrollen zuweisen	SharePoint Online Berechtigungen in Systemrollen aufnehmen auf Seite 83
Geschäftsrollen zuweisen	SharePoint Online Berechtigungen an Geschäftsrollen zuweisen auf Seite 82
Organisationen zuweisen	SharePoint Online Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 80
SharePoint Online Rollen ausschließen	Wirksamkeit von SharePoint Online Rollen auf Seite 129
Zusatzeigenschaften zuweisen	Zusatzeigenschaften an SharePoint Online Gruppen zuweisen auf Seite 115
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 36

Überblick über eine SharePoint Online Rolle

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 89 beschriebene Verhalten können Sie auch für SharePoint Online Rollen nutzen.

Die Wirksamkeit der Zuweisungen wird in den Tabellen 03UserHas03SRLAssign und BaseTreeHas03SRLAssign über die Spalte XIsInEffect abgebildet.

Voraussetzungen

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

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. Compianceregeln 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

Dafür stellt der One Identity Manager Standard-Berechnungsvorschriften bereit. Im Web Portal können die Berechnungsvorschriften modifiziert werden.

- Berichte und Statistiken

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

- *One Identity Manager Anwenderhandbuch für das Web Portal*
- *One Identity Manager Administrationshandbuch für Attestierungen*
- *One Identity Manager Administrationshandbuch für Compianceregeln*
- *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 [133](#).

- Zielsystemtypen

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

Weitere Informationen finden Sie unter [Ausstehende Objekte nachbehandeln](#) auf Seite [37](#).

- Kontendefinitionen

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

Weitere Informationen finden Sie unter [Kontendefinitionen für SharePoint Online Benutzerkonten](#) auf Seite [43](#).

- Server

Für die Verarbeitung der SharePoint Online-spezifischen 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 [133](#).

- Zielsystemverantwortliche

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

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

Weitere Informationen finden Sie unter [Zielsystemverantwortliche](#) auf Seite 139.

SharePoint Online Authentifizierungsmodi

Für den Authentifizierungsmodus werden folgende Stammdaten geliefert.

Tabelle 33: 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 Anmeldeame	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.

Jobserver für SharePoint Online-spezifische Prozessverarbeitung

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

- Erstellen Sie im Designer in der Kategorie **Basisdaten | Installationen | Jobserver** einen Eintrag für den Jobserver. Ausführliche Informationen dazu finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Wählen Sie im Manager in der Kategorie **SharePoint 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

- [Stammdaten eines Jobservers](#) auf Seite 135
- [Festlegen der Serverfunktionen](#) auf Seite 137

Verwandte Themen

- [Systemanforderungen für den Synchronisationsserver](#) auf Seite 15

SharePoint Online Jobserver bearbeiten

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

- [Stammdaten eines Jobserver](#) auf Seite 135
- [Festlegen der Serverfunktionen](#) auf Seite 137

Stammdaten eines 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 34: Eigenschaften eines Jobserver

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobserver.
Vollständiger Servername	Vollständiger Servername gemäß DNS Syntax. Beispiel: <Name des Servers>.<Vollqualifizierter Domänenname>
Server ist Cluster	Angabe, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. HINWEIS: Die Eigenschaften Server ist Cluster und Server gehört zu Cluster schließen einander aus.
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.
IP-Adresse (IPv4)	Internet Protokoll Version 4 (IPv4)-Adresse des Servers.
Kopierverfahren (Zielservers)	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 Jobserver.
Ausführender Server	Bezeichnung des ausführenden Servers. Eingetragen wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden. Diese Angabe wird bei der automatischen Aktualisierung des One Identity Manager Service ausgewertet. Verarbeitet ein Server mehrere Queues, wird mit der Auslieferung von Prozessschritten solange gewartet, bis alle Queues, die auf demselben Server

Eigenschaft	Bedeutung
Queue	<p>abgearbeitet werden, die automatische Aktualisierung abgeschlossen haben.</p> <p>Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.</p>
Serverbetriebssystem	<p>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.</p>
Angaben zum Dienstkonto	<p>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.</p>
One Identity Manager Service installiert	<p>Angabe, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur QBM_PJobQueueLoad aktiviert, sobald die Queue das erste Mal angefragt wird.</p> <p>Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.</p>
Stopp One Identity Manager Service	<p>Angabe, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten.</p> <p>Den Dienst können Sie mit entsprechenden administrativen Rechten im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im <i>One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche</i>.</p>
Kein automatisches Softwareupdate	<p>Angabe, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist.</p> <p>HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.</p>
Softwareupdate läuft	<p>Angabe, ob gerade eine Softwareaktualisierung ausgeführt wird.</p>

Eigenschaft	Bedeutung
Letzter Abrufzeitpunkt	Zeitpunkt der letzten Prozessabholung.
Letzte Timeout Prüfung	Zeitpunkt der letzten Prüfung für geladene Prozessschritte, deren Auslieferung den Wert im Konfigurationsparameter Common Jobservice LoadedJobsTimeOut überschreitet.
Serverfunktion	Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

Verwandte Themen

- [Festlegen der Serverfunktionen](#) auf Seite 137

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 35: 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

Serverfunktion	Anmerkungen
	<p>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.</p> <p>Bei der initialen Schemainstallation wird der Server, auf dem die One Identity Manager-Datenbank installiert ist, mit dieser Serverfunktion gekennzeichnet.</p>
SQL Ausführungsserver	Der Server kann SQL Aufträge ausführen. Für eine Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.
CSV Skriptserver	Der Server kann CSV-Dateien per Prozesskomponente ScriptComponent verarbeiten.
Nativer Datenbankkonnektor	Der Server kann sich mit einer ADO.Net Datenbank verbinden.
One Identity Manager-Datenbankkonnektor	Server, auf dem der One Identity Manager Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem One Identity Manager aus.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
Primärer Domänen-Controller	Primärer Domänen-Controller.
Profilservers	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

- [Stammdaten eines Jobserver](#)s auf Seite 135

Zielsystemverantwortliche

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

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

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

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

1. Der One Identity Manager Administrator legt Personen als Zielsystemadministratoren fest.
2. Die Zielsystemadministratoren nehmen die Personen in die Standardanwendungsrolle für die Zielsystemverantwortlichen auf.
Zielsystemverantwortliche der Standardanwendungsrolle sind berechtigt alle Mandanten im One Identity Manager zu bearbeiten.
3. Zielsystemverantwortliche können innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche berechtigen und bei Bedarf weitere untergeordnete Anwendungsrollen erstellen und einzelnen Mandanten zuweisen.

Tabelle 36: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	<p>Die Zielsystemverantwortlichen müssen der Anwendungsrolle Zielsysteme SharePoint Online oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Übernehmen die administrativen Aufgaben für das Zielsystem.• Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen.• Bearbeiten Kennwortrichtlinien für das Zielsystem.• Bereiten Gruppen zur Aufnahme in den IT Shop vor.• Können Personen anlegen, die eine andere Identität

Benutzer

Aufgaben

haben als den Identitätstyp **Primäre Identität**.

- Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.
- Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation.
- Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Um initial Personen als Zielsystemadministrator festzulegen

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

Um initial Personen in die Standardanwendungsrolle für Zielsystemverantwortliche aufzunehmen

1. Melden Sie sich als Zielsystemadministrator (Anwendungsrolle **Zielsysteme | Administratoren**) am Manager an.
2. Wählen Sie die Kategorie **One Identity Manager Administration | Zielsysteme | SharePoint 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

Konfigurationsparameter für die Verwaltung einer SharePoint Online

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

Tabelle 37: 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.
TargetSystem SharePointOnline Accounts	Parameter zur Konfiguration der Angaben zu SharePoint Online Benutzerkonten.
TargetSystem SharePointOnline Accounts MailTemplateDefaultValues	Der Konfigurationsparameter enthält die Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage Person - Erstellung neues Benutzerkonto mit Standardwerten verwendet.
TargetSystem SharePointOnline DefaultAddress	Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem SharePointOnline MaxFullsyncDuration	Der Konfigurationsparameter enthält die maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.

Konfigurationsparameter Bedeutung

TargetSystem |
SharePointOnline |
PersonAutoDefault

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

TargetSystem |
SharePointOnline |
PersonAutoFullsync

Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.

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.

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

Tabelle 38: 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

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

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 39: Zulässige Verarbeitungsmethoden für Objekttypen

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

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 Geschäftssagilität 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

A

Architekturüberblick 8
Ausschlussdefinition 89, 129
Ausstehendes Objekt 37
Authentifizierung
 Authentifizierungsmodus 133
Authentifizierungsmodus 133
Authentifizierungsobjekt 68
Automatisierungsgrad
 bearbeiten 47

B

Basisobjekt 31
Benutzerkonto 68, 100
 administratives Benutzerkonto 72
 Administrator 102, 105
 Anmeldename 102, 105
 Auditor 102, 105
 Authentifizierungsobjekt 68, 102, 105
 Authentifizierungssystem 102, 105
 Automatisierungsgrad 66
 bearbeiten 101
 Berechtigung zuweisen 87
 Bildungsregeln ausführen 53
 erstellen 101
 Gruppen zuweisen 87
 Gruppenidentität 72, 74
 Identität 70, 102, 105
 Kategorie 91
 Kategorie zuordnen 102, 105

löschen 109
Löschverzögerung 109
mehrere je Person 68
Person zuordnen 62, 102
persönliche
 Administratoridentität 72-73
privilegiertes Benutzerkonto 70, 75, 102, 105
Risikoindex 102, 105
Rolle zuweisen 87
Rollenzuweisung 125
sperrern 109
Standardbenutzerkonto 71
Typ 70-72, 75
Überblick 108
verbunden 67
wiederherstellen 109
Zusatzeigenschaft zuweisen 109
Benutzerpräfix 133
Berechtigung
 ausschließen 89
 Benutzerkonto zuweisen 86
 Geschäftsrolle zuweisen 82
 Gruppe 79
 in IT Shop aufnehmen 84
 Organisationen zuweisen 80
 Rolle 79
 Systemrolle zuweisen 83
 Übersicht aller Zuweisungen 94
 Vererbung über Systemrollen 83
 wirksam 89

Berechtigungsstufe 115-117
 an Benutzerkonten zuweisen 116
 an Gruppen zuweisen 116
 löschen 117
 Rollendefinition 125
 Website 116
 Websitesammlung 115, 117

Berechtigungszuweisung
 direkt 86-87

Bildungsregel
 IT Betriebsdaten ändern 53

D

Dummy-Person 74

E

Einzelobjekt synchronisieren 36
Einzelobjektsynchronisation 31, 36
 beschleunigen 32

G

Gruppe
 Abteilung zuweisen 80
 arbeiten 112
 ausschließen 89
 Benutzerkonto zuweisen 79, 86
 Eigentümer 112
 einrichten 110
 erstellen 111
 Geschäftsrolle zuweisen 82
 in IT Shop aufnehmen 84
 Kategorie 91
 Kategorie zuordnen 112
 Kostenstelle zuweisen 80

löschen 115
Risikoindex 112
Rollenzuweisung 125
SharePoint Online Rolle zuweisen 87
Standort zuweisen 80
Systemrolle zuweisen 83
 über IT Shop bestellen 112
Überblicksformular 114
Übersicht aller Zuweisungen 94
Vererbung über Kategorien 120
Vererbung über Rollen 79
Vererbung über Systemrollen 83
wirksam 89
 Zusatzeigenschaft zuweisen 115

Gruppenidentität 72, 74

Gruppenpräfix 133

I

Identität 70
IT Betriebsdaten
 ändern 53
IT Shop Regal
 Gruppen zuweisen 84
 Kontendefinitionen zuweisen 57
 Rolle zuweisen 84

J

Jobserver
 bearbeiten 16
 Eigenschaften 135
 Lastverteilung 32

K

Kategorie 120

Konfigurationsparameter 11, 142
Kontendefinition 43

- an Abteilung zuweisen 55
- an alle Personen zuweisen 56
- an Benutzerkonten zuweisen 67
- an Geschäftsrolle zuweisen 55
- an Kostenstelle zuweisen 55
- an Kunden-Umgebung zuweisen 59
- an Person zuweisen 54, 56
- an Standort zuweisen 55
- an Systemrollen zuweisen 57
- automatisch zuweisen 56
- Automatisierungsgrad 48
- Automatisierungsgrad bearbeiten 47
- bearbeiten 44
- erstellen 44
- in IT Shop aufnehmen 57
- IT Betriebsdaten 50-51
- löschen 59

Kunden-Umgebung

- Kontendefinition (initial) 59

L

Lastverteilung 32

M

Mitgliedschaft

- Änderung provisionieren 29

N

NLog 40

O

Objekt

- ausstehend 37
- publizieren 37
- sofort löschen 37

P

Person

- Benutzerkonto zuweisen 68
- Gruppenidentität 74
- Hauptidentität 73
- persönliche Administratoridentität 73
- primäre Identität 74

Personenzuordnung

- entfernen 65
- manuell 65
- Suchkriterium 63

Persönliche Administratoridentität 72-73
Präfix 133

- Website erstellen 123

Produkt und SKU

- Geschäftsrolle zuweisen 82
- Übersicht aller Zuweisungen 94

Projektvorlage 144
Protokolldatei 40
Provisionierung

- beschleunigen 32
- Mitgliederliste 29

R

Revision zurücksetzen 40

Rolle

- Abbildung im One Identity Manager 126
 - Abteilung zuweisen 80
 - ausschließen 129
 - Benutzerkonto zuweisen 79, 86
 - Berechtigung vererben 125
 - Berechtigungsstufe 125-126
 - Gruppe zuweisen 88
 - in IT Shop aufnehmen 84
 - Kostenstelle zuweisen 80
 - Rollenzuweisung 88, 125
 - Standort zuweisen 80
 - Systemrolle zuweisen 83
 - über IT Shop bestellen 126-127
 - Überblick 128
 - Vererbung über Rollen 79
 - Vererbung über Systemrollen 83
 - Website 126-127
 - wirksam 129
- Root-Site 122
- Website 122
 - Websitesammlung 119

S

Schema

- aktualisieren 28
- Änderungen 28
- komprimieren 28

Serverfunktion 137

SharePoint Online Konnektor 8

SharePoint Online Mandant

- Überblick 99
- Zielsystemverantwortlicher 139

SharePoint Online Server 8

Standardbenutzerkonto 71

Startinformation zurücksetzen 40

Synchronisation

- konfigurieren 20-21, 26
- Scope 26
- simulieren 40
- starten 20-21, 34
- Synchronisationsprojekt
 - erstellen 20-21
- Variable 26
- Verbindungsparameter 20-21, 26
- verhindern 36
- Voraussetzung 12
- Workflow 20-21, 28
- Zeitplan 34

Synchronisationsanalysebericht 40

Synchronisationskonfiguration

- anpassen 26, 28

Synchronisationsprojekt

- bearbeiten 99
- deaktivieren 36
- erstellen 20-21
- Projektvorlage 144

Synchronisationsprotokoll 35, 40

- erstellen 25

- Inhalt 25

Synchronisationsrichtung

- In das Zielsystem 20-21, 28
- In den Manager 20-21

Synchronisationsserver 8, 15

- bearbeiten 133-134
- installieren 16
- Jobserver 16
- konfigurieren 15
- Serverfunktion 137

- Systemanforderungen 15
- Synchronisationsworkflow
 - erstellen 20-21, 28
- System
 - bearbeiten 96
 - Kontendefinition 97
 - Personenzuordnung 63
 - Synchronisationsart 97

U

- URL
 - Website 123-124
 - Websitesammlung 119-120

W

- Website 122
 - anonymer Zugriff 122
 - Autor 122
 - Präfix 123
 - Rollendefinition 122
 - Rollenzuweisung 122, 125
 - Root-Site 122
 - Berechtigungen vererben 125
 - untergeordnete 125
 - URL 123-124
 - öffnen 124
 - Webvorlage 124
- Websitesammlung 118
 - Administrator 119
 - Kategorie 91
 - Kategorien festlegen 120
 - Kontendefinition 119
 - Root-Site 119
 - Berechtigungen vererben 125

- Server 119
- Überblick 121
- URL 119-120

- Webvorlage
 - Website erstellen 124

Z

- Zeitplan 34
 - deaktivieren 36
- Zielsystemabgleich 37
- Zielsystemverantwortlicher 139
 - festlegen 97
- Zusatzeigenschaft
 - Benutzerkonto 109
 - Gruppe zuweisen 115