



One Identity Manager 8.0.2

Administrationshandbuch für die
Anbindung einer SharePoint Online-
Umgebung

Copyright 2018 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 Eigentumsrechts 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 GEWÄHRLEISTUNGEN 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 mögliche Personen- oder Sachschäden oder Schaden mit Todesfolge hin.
-  **VORSICHT:** Das Symbol **VORSICHT** weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.
-  **WICHTIG, HINWEIS, TIPP, MOBIL, or VIDEO:** Ein Informationssymbol weist auf Begleitinformationen hin.

Inhalt

Verwalten einer SharePoint Online-Umgebung	5
Architekturüberblick	5
One Identity Manager Benutzer für die Verwaltung einer SharePoint Online-Umgebung	6
Einrichten der Synchronisation mit einer SharePoint Online-Umgebung	8
Hinweise zur Synchronisation von SharePoint Online Websitesammlungen	9
Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung	10
Einrichten des Synchronisationsservers	12
Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer SharePoint Online-Umgebung	15
Synchronisationsergebnisse anzeigen	21
Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen	22
Anpassen einer Synchronisationskonfiguration	23
Synchronisation in die SharePoint Online-Umgebung konfigurieren	24
Schema aktualisieren	25
Nachbehandlung ausstehender Objekte	26
Provisionierung von Mitgliedschaften konfigurieren	28
Unterstützung bei der Analyse von Synchronisationsproblemen	29
Deaktivieren der Synchronisation	30
Basisdaten für die Verwaltung einer SharePoint Online-Umgebung	31
Einrichten von Kontendefinitionen	32
Erstellen einer Kontendefinition	32
Stammdaten einer Kontendefinition	33
Erstellen der Automatisierungsgrade	35
Stammdaten eines Automatisierungsgrades	37
Erstellen einer Abbildungsvorschrift für IT Betriebsdaten	38
Erfassen der IT Betriebsdaten	39
Ändern der IT Betriebsdaten	41
Zuweisen der Kontendefinition an Personen	42
Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen	43
Kontendefinition an Geschäftsrollen zuweisen	43

Kontendefinition an alle Personen zuweisen	44
Kontendefinition direkt an Personen zuweisen	45
Kontendefinition an Systemrollen zuweisen	45
Kontendefinition in den IT Shop aufnehmen	46
Zuweisen der Kontendefinition an ein Zielsystem	47
Löschen einer Kontendefinition	47
Zielsystemverantwortliche	49
Anhang: Konfigurationsparameter für die Verwaltung einer SharePoint Online-Umgebung	52
Anhang: Standardprojektvorlage für SharePoint Online	54
Anhang: Verarbeitung von Systemobjekten	55
Über uns	56
Kontaktieren Sie uns	56
Technische Supportressourcen	56
Index	57

Verwalten einer SharePoint Online-Umgebung

Die Verwaltung einer SharePoint Online-Umgebung mit dem One Identity Manager konzentriert sich auf die Abbildung von Websitesammlungen, Websites und Gruppen die in einer Cloud-Umgebung liegen.

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

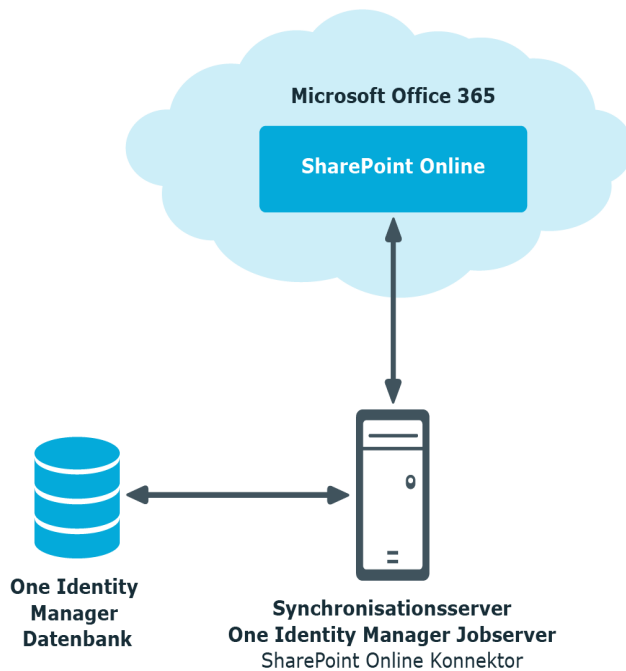
- [Anhang: Verarbeitung von Systemobjekten](#)

Architekturüberblick

Um auf die Daten einer SharePoint Online-Organisation 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 Microsoft Office 365 Abonnements des SharePoint Online in der Cloud. Die Microsoft CSOM (Client-side object model) Bibliothek wird für den Zugriff auf die SharePoint Online Daten verwendet.

Für den Zugriff auf die Daten einer SharePoint Online-Organisation, muss das Zielsystem Azure Active Directory in dem die Organisation sich befindet, synchronisiert werden.

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	<p>Die Zielsystemadministratoren müssen der Anwendungsrolle Zielsysteme Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen. • Legen die Zielsystemverantwortlichen fest. • Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein.

Benutzer	Aufgaben
Zielsystemverantwortliche	<ul style="list-style-type: none"> • Legen sich fest, welche Anwendungsrollen für Zielsystemverantwortliche sich widersprechen. • Berechtigen weitere Personen als Zielsystemadministratoren. • Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme. <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 zur Aufnahme in den IT Shop vor. • 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	<ul style="list-style-type: none"> • 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.

Einrichten der Synchronisation mit 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. Voraussetzungen für die Synchronisation sind:

- Die Synchronisation der Azure Active Directory-Umgebung wird regelmäßig ausgeführt.
- Der Azure Active Directory Mandant ist im One Identity Manager bekannt.
- Die Administratoren der zu synchronisierenden Websitesammlungen sind im Synchronisationsprojekt entsprechend angepasst.

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.
2. Die One Identity Manager Bestandteile für die Verwaltung von SharePoint Online-Umgebungen sind verfügbar, wenn der Konfigurationsparameter "TargetSystem\SharePoint Online" 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 10
- [Einrichten des Synchronisationservers](#) auf Seite 12
- [Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer SharePoint Online-Umgebung](#) auf Seite 15
- [Deaktivieren der Synchronisation](#) auf Seite 30
- [Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen](#) auf Seite 22
- [Hinweise zur Synchronisation von SharePoint Online Websitesammlungen](#)
- [Anpassen einer Synchronisationskonfiguration](#) auf Seite 23
- [Anhang: Konfigurationsparameter für die Verwaltung einer SharePoint Online-Umgebung](#) auf Seite 52
- [Anhang: Standardprojektvorlage für SharePoint Online](#) auf Seite 54

Hinweise zur Synchronisation von SharePoint Online Websitesammlungen

Für die Synchronisation der Websitesammlungen SharePoint Online-Umgebung beachten Sie folgende Hinweise:

- Das Mapping für SharePoint Online Websitesammlungen ist Bestandteil der SharePoint Online Projektvorlage. Die Synchronisation der SharePoint Online Websitesammlungen übernimmt der SharePoint Online Konnektor.
- Benötigt wird ein administratives Benutzerkonto der zugehöriger Azure Active Directory Organisation.
 - ❗ **HINWEIS:** Dieses Benutzerkonto muss an allen zu administrierenden Websitesammlungen als Websitesammlungsadministrator eingetragen werden. Dies nehmen Sie im SharePoint Online vor.

Um den Namen der Azure Active Directory Organisation zu ermitteln

1. Melden Sie sich am Office 365 Admin Portal an.
2. Wählen Sie **Domänen** unter der Kategorie **Setup** im linken Menü aus.
3. Der Organisationsname ist Bestandteil des Domänennamens. Zum Beispiel: "<Organisationsname>.onmicrosoft.com".

Benutzername und Kennwort sind die Zugangsdaten des Benutzerkontos des Azure Active Directory Administrators der Organisation. Der Benutzername ist dabei eine E-Mail Adresse: <Benutzername>@<Organisationsname>.onmicrosoft.com.

- Beim initialen Einrichten der Systemverbindung der SharePoint Online

Synchronisation mit dem Synchronization Editor, muss der Synchronisationsbenutzer einen der Administratoren der zu administrierender Websitesammlungen im SharePoint Online beziehungsweise einen Azure Active Directory Organisationsadministrator.

- Die folgende Synchronisationsreihenfolge ist zwingend einzuhalten:
 1. Azure Active Directory
 2. SharePoint Online

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 einer SharePoint Online-Umgebung mit der ausgelieferten One Identity Manager Standardkonfiguration stellen Sie ein Benutzerkonto bereit, das die folgenden Berechtigungen besitzt.</p> <ul style="list-style-type: none">• Administrator alle zu administrierenden Websitesammlungen.
Benutzerkonto des One Identity Manager Service	<p>Das Benutzerkonto für den One Identity Manager Service benötigt die Rechte, um die Operationen auf Dateiebene durchzuführen (Rechtevergabe, Verzeichnisse und Dateien anlegen und bearbeiten).</p> <p>Das Benutzerkonto muss der Gruppe "Domänen-Benutzer" (Domain Users) angehören.</p> <p>Das Benutzerkonto benötigt das erweiterte Benutzerrecht "Anmelden als Dienst" (Log on as a service).</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 Kommandozeilenaufwurf vergeben:</p> <pre>netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/user="NT AUTHORITY\NETWORKSERVICE"</pre>

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

Erläuterungen zu den erforderlichen Rechten

Die Websitesammlungen in den das Benutzerkonto für die Synchronisation als Administrator eingetragen werden soll, sind:

- alle zu synchronisierende Websitesammlungen.

Um Berechtigungen über das Microsoft Online Portal zuzuweisen

1. Navigieren Sie zu <https://portal.microsoftonline.com/> und melden Sie sich als Administrator an.
Damit wechseln Sie zur Office 365 Begrüßungsseite.
2. Klicken Sie die **Administrator** Kachel um das Microsoft Office 365 Admin Center zu öffnen.
3. Wählen Sie aus dem Menü auf der linken Seite, **Admin Centers | SharePoint**.
Damit wechseln Sie zum SharePoint Admin Center.
4. Klicken Sie auf **Websitesammlungen** im Menü auf der linken Seite.
5. Klicken Sie im Kontrollkasten neben die zu administrierende Websitesammlung um sie auszuwählen.
6. Wählen Sie in der Werkzeugleiste unter dem Menü **Besitzer** den Eintrag **Administratoren verwalten**.
7. Bestätigen Sie dass das Azure Active Directory Benutzerkonto als Websitesammlungadministrator eingetragen ist.

- ODER -

Fügen Sie das gewünschte Azure Active Directory Benutzerkonto ein.

Ausführliche Information zur Azure Active Directory finden Sie in der Azure Active Directory Dokumentation von Microsoft.

8. Wiederholen Sie die Schritte 5 bis 7 für alle zu administrierenden Websitesammlungen.

Einrichten des Synchronisationsservers

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

- Windows Betriebssystem
Unterstützt werden die Versionen:
 - Windows Betriebssystem ab Version 8.1
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016
- Microsoft .NET Framework Version 4.5.2 oder höher
 - ❗ **HINWEIS:** Microsoft .NET Framework Version 4.6.0 wird nicht unterstützt.
 - ❗ **HINWEIS:** Beachten Sie die Empfehlungen des Zielsystemherstellers.
- Windows Management Framework 4.0
- One Identity Manager Service, SharePoint Online Konnektor
 - Installieren Sie die One Identity Manager Komponenten mit dem Installationsassistenten.
 1. Wählen Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen**.
 2. Wählen Sie die Maschinenrolle **Server | Jobserver | SharePoint 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. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein.

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

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

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

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

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 und klicken Sie **Weiter**.
3. Auf der Seite **Servereigenschaften** legen Sie fest, auf welchem Server der One Identity Manager Service installiert werden soll.
 - a. Wählen Sie in der Auswahlliste **Server** einen Jobserver aus.
- ODER -
Um einen neuen Jobserver zur erstellen, klicken Sie **Hinzufügen**.
 - b. Bearbeiten Sie folgende Informationen für den Jobserver.

Tabelle 3: Eigenschaften eines Jobservers

Eigenschaft	Beschreibung
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. Beispiel: <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** legen Sie fest, welche Rolle der Jobserver im One Identity Manager übernimmt. Abhängig von der gewählten Maschinenrolle werden die Installationspakete ermittelt, die auf dem Jobserver installiert werden.

Wählen Sie mindestens folgende Rollen:

- SharePoint Online

5. Auf der Seite **Serverfunktionen** legen Sie die Funktion des Servers in der One Identity Manager-Umgebung fest. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

Die Serverfunktionen sind abhängig von den gewählten Maschinenrollen bereits ausgewählt. Sie können die Serverfunktionen hier weiter einschränken.

Wählen Sie mindestens folgende Serverfunktionen:

- SharePoint Online Konnektor

6. Auf der Seite **Dienstkonfiguration** 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.

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.

Tabelle 4: Installationsinformationen

Eingabe	Beschreibung
Computer	Server, auf dem der Dienst installiert und gestartet wird. Um einen Server auszuwählen <ul style="list-style-type: none">• Erfassen Sie den Servernamen. -ODER-• Wählen Sie einen Eintrag in der Liste.

Eingabe	Beschreibung
Dienstkonto	<p>Angaben zum Benutzerkonto des One Identity Manager Service.</p> <p>Um ein Benutzerkonto für den One Identity Manager Service zu erfassen</p> <ul style="list-style-type: none"> Erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung. <p>Als Benutzerkonto für den One Identity Manager Service muss das Serverfarmkonto der SharePoint Farm genutzt werden.</p>
Installationskonto	<p>Angaben zum administrativen Benutzerkonto für die Installation des Dienstes.</p> <p>Um ein administratives Benutzerkonto für die Installation zu erfassen</p> <ul style="list-style-type: none"> Aktivieren Sie die Option Erweitert. Aktivieren Sie die Option Angemeldeter Benutzer. Es wird das Benutzerkonto des aktuell angemeldeten Benutzers verwendet. - ODER - Geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.

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: Der Dienst wird mit der Bezeichnung "One Identity Manager Service" in der Dienstverwaltung des Servers eingetragen.

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer SharePoint Online-Umgebung

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

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

Voraussetzungen für die Erstellung eines Synchronisationsprojektes

- Die Synchronisation der Azure Active Directory-Umgebung wird regelmäßig ausgeführt.
- Der Azure Active Directory Mandant ist im One Identity Manager bekannt.
- Die Administratoren der zu synchronisierenden Websitesammlungen sind im Synchronisationsprojekt entsprechend angepasst.

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

Tabelle 5: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Benutzername und Kennwort zur Anmeldung	Benutzerkonto und Kennwort zur Authentifizierung am SharePoint Online. Beispiel: <Benutzername des Synchronisationsnutzers>@yourorganisation.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 10.
Synchronisationsserver für SharePoint Online	Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem SharePoint Online Konnektor installiert sein.

Tabelle 6: Zusätzliche Eigenschaften für den Jobserver

Eigenschaft	Wert
Serverfunktion	SharePoint Online Konnektor
Maschinenrolle	Server/Jobserver/SharePointOnline

Weitere Informationen finden Sie unter [Einrichten des Synchronisationsservers](#) auf Seite 12.

Verbindungsdaten zur One Identity Manager	SQL Server:
---	-------------

Angaben

Erläuterungen

Datenbank

- Datenbankserver
- Datenbank
- Datenbankbenutzer 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.

Oracle:

- Angabe, ob der Zugriff direkt oder über Oracle Client erfolgt

Die erforderlichen Verbindungsdaten sind abhängig von der Einstellung dieser Option.

- Datenbankserver
- Port der Oracle Instanz
- Service Name
- Oracle Datenbankbenutzer und Kennwort
- Datenquelle (TNS Alias Name aus der TNSNames.ora)

Remoteverbindungsserver

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

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

Konfiguration des Remoteverbindungservers:

- 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

Jobserver benötigt.

TIPP: Der Remoteverbindungsserver benötigt dieselbe Konfiguration (bezüglich der installierten Software) 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.

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

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

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

Um ein initiales Synchronisationsprojekt für eine SharePoint Online-Umgebung 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**. 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 **Verbindungsparameter** erfassen Sie die Anmeldeinformationen für die Verbindung zum SharePoint Online.

Tabelle 7: Verbindungsparameter zum SharePoint Online

Eigenschaft	Beschreibung
Organisationsname	Der Name Ihrer Organisation.
Benutzername (user@-domain)	Vollqualifizierter Name (FQDN) des Benutzerkonto zur Anmeldung. Beispiel: <code><user>@<domain.com></code> <code>sync.user@yourorganisation.onmicrosoft.com</code> Deiner Organisationsname wird automatisch eingefügt.
Kennwort	Kennwort zum Benutzerkonto.

Klicken Sie **Weiter**.

5. Klicken Sie danach **Fertig** um zurück zum Projektassistent zu gehen.
6. Der Assistent lädt das Zielsystemschemata. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.
7. Auf der Seite **Zielsystemzugriff einschränken** legen Sie fest, wie der Systemzugriff erfolgen soll. Zur Auswahl stehen:


Tabelle 8: Zielsystemzugriff festlegen

Option	Bedeutung
Das Zielsystem soll nur eingelesen werden.	Angabe, ob nur ein Synchronisationsworkflow zum initialen Einlesen des Zielsystems in die One Identity Manager Datenbank eingerichtet werden soll. Der Synchronisationsworkflow zeigt folgende Besonderheiten: <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	Angabe, ob zusätzlich zum Synchronisationsworkflow zum initialen Einlesen des Zielsystems ein Provisionierungsworkflow eingerichtet werden soll.

Option	Bedeutung
durchgeführt werden.	<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.

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

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

- Klicken Sie , um einen neuen Jobserver anzulegen.
- Erfassen Sie die Bezeichnung des Jobservers und den vollständigen Servernamen gemäß DNS-Syntax.
- Klicken Sie **OK**.

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

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

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

Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

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 Synchronisation Editor.

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

1. Um das Synchronisationsprotokoll für die Zielsystemverbindung zu konfigurieren, wählen Sie die Kategorie **Konfiguration | Zielsystem**.
2. Um das Synchronisationsprotokoll für die Datenbankverbindung zu konfigurieren, wählen Sie die Kategorie **Konfiguration | One Identity Manager Verbindung**.
3. Wählen Sie den Bereich **Allgemein** und klicken Sie **Konfigurieren...**
4. Wählen Sie den Bereich **Synchronisationsprotokoll** und aktivieren Sie **Synchronisationsprotokoll erstellen**.

5. 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.

6. Klicken Sie **OK**.

Um regelmäßige Synchronisationen auszuführen

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

Um die initiale Synchronisation manuell zu starten

1. Wählen Sie die Kategorie **Konfiguration | Startkonfigurationen**.
2. Wählen Sie in der Dokumentenansicht eine Startkonfiguration und klicken Sie **Ausführen**.
3. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

HINWEIS: Beachten Sie bei der Einrichtung der Synchronisation die unter [Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen](#) auf Seite 22 beschriebenen Empfehlungen.

Verwandte Themen

- [Einrichten des Synchronisationsservers](#) auf Seite 12
- [Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung](#) auf Seite 10
- [Synchronisationsergebnisse anzeigen](#) auf Seite 21
- [Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen](#) auf Seite 22
- [Anpassen einer Synchronisationskonfiguration](#) auf Seite 23
- [Anhang: Standardprojektvorlage für SharePoint Online](#) auf Seite 54

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. Wählen Sie die Kategorie **Protokolle**.
2. Klicken Sie in der Symbolleiste der Navigationsansicht ►.
In der Navigationsansicht werden die Protokolle aller abgeschlossenen Synchronisationsläufe angezeigt.
3. 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. Wählen Sie die Kategorie **Protokolle**.
2. Klicken Sie in der Symbolleiste der Navigationsansicht ⚡.
In der Navigationsansicht werden die Protokolle aller abgeschlossenen Provisionierungsprozesse angezeigt.
3. 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.

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.

Besonderheiten zur Synchronisation von SharePoint Online-Umgebungen

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

Mehrfache Organisationen nicht unterstützt

Standardmäßig, gibt es nur einen Azure Active Directory Mandant pro Synchronisationsprojekt. Dieser Mandant entspricht die Organisation für die Anmeldung an Microsoft Office 365. Das Zielsystemschemata in One Identity Manager lässt sich nicht erweitern.

Zielsystem Scope einstellen

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

Der Scope darf nur die Websitesammlungen umfassen, in denen das 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 Websammlungen nur die, in denen der Synchronisationsbenutzer dem Administrator der SharePoint Online-Umgebung entspricht.

Verwandte Themen

- [Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Online-Umgebung](#) auf Seite 10

Anpassen einer Synchronisationskonfiguration

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

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

- 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.

- Um festzulegen, welche SharePoint Online Objekte und Datenbankobjekte bei der Synchronisation behandelt werden, bearbeiten Sie den Scope der Zielsystemverbindung und der One Identity Manager-Datenbankverbindung. Um Dateninkonsistenzen zu vermeiden, definieren Sie in beiden Systemen den gleichen Scope. Ist kein Scope definiert, werden alle Objekte synchronisiert.
- Wenn sich das One Identity Manager Schema oder das Zielsystemschemata geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.

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

- Wenn eine weitere Synchronisation mit derselben Startkonfiguration gestartet wird, wird dieser Prozess gestoppt und erhält den Ausführungsstatus "Frozen". Es wird eine Fehlermeldung in die Protokolldatei des One Identity Manager Service geschrieben.
- 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. Gruppieren Sie die Startkonfigurationen mit gleichem Startverhalten.

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

Detaillierte Informationen zum Thema

- [Synchronisation in die SharePoint Online-Umgebung konfigurieren](#) auf Seite 24
- [Schema aktualisieren](#) auf Seite 25

Synchronisation in die SharePoint Online-Umgebung konfigurieren

Das Synchronisationsprojekt für die initiale Synchronisation stellt je einen Workflow zum initialen Einlesen der (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 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.

Nachbehandlung ausstehender Objekte

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

Objekte, die als ausstehend gekennzeichnet wurden,

- können im One Identity Manager nicht bearbeitet werden,
- werden bei jeder weiteren Synchronisation ignoriert,
- müssen im One Identity Manager einzeln nachbearbeitet werden.

Führen Sie dafür einen Zielsystemabgleich durch.

Um ausstehende Objekte nachzubearbeiten




1. Wählen Sie in der Navigationsansicht die Tabelle, für die sie ausstehende Objekte nachbearbeiten möchten.
Das Formular für den Zielsystemabgleich wird geöffnet. Hier werden alle Objekte angezeigt, die als ausstehend markiert sind.

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**.
2. Wählen Sie die Objekte, die Sie nachbearbeiten möchten. Mehrfachauswahl ist möglich.
 3. Klicken Sie in der Formularelementeiste eins der folgenden Symbole, um die jeweilige Methode auszuführen.

Tabelle 9: Methoden zur Behandlung ausstehender Objekte

Symbol	Methode	Beschreibung
	Löschen	Das Objekt wird sofort in der One Identity Manager Datenbank gelöscht. Eine Löschverzögerung wird nicht berücksichtigt. Die Markierung "Ausstehend" wird für das Objekt entfernt. Indirekte Mitgliedschaften können nicht gelöscht werden.
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung "Ausstehend" wird für das Objekt entfernt. Die Methode löst das Ereignis "HandleOutstanding" aus. Dadurch wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt. Voraussetzungen: <ul style="list-style-type: none">• Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen.• Der Zielsystemkonnektor kann schreibend auf das Zielsystem zugreifen.
	Zurücksetzen	Die Markierung "Ausstehend" wird für das Objekt entfernt.

4. 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 Formularelementeiste .

Um kundenspezifische Tabellen in den Zielsystemabgleich aufzunehmen

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

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

Provisionierung von Mitgliedschaften konfigurieren

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

- Mitgliedschaften werden im Zielsystem in Form einer Liste als Eigenschaft eines Objekts gespeichert.
- 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. Starten Sie den Manager.
2. Wählen Sie die Kategorie **SharePoint Online | Basisdaten zur Konfiguration | Zielsystemtypen**.
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.

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

Unterstützung bei der Analyse von Synchronisationsproblemen

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

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

Um den Synchronisationsanalysebericht zu erstellen

1. Wählen Sie das Menü **Hilfe | Synchronisationsanalysebericht erstellen** und beantworten Sie die Sicherheitsabfrage mit **Ja**.

Die Generierung des Berichts nimmt einige Zeit in Anspruch. Er wird in einem separaten Fenster angezeigt.

2. Drucken Sie den Bericht oder Speichern Sie ihn in einem der verschiedenen Ausgabeformate.

Deaktivieren der Synchronisation

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

Um regelmäßige Synchronisationen zu verhindern

- 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 geladene Synchronisationsprojekt zu deaktivieren

1. Wählen Sie auf der Startseite die Ansicht **Allgemein**.
2. Klicken Sie **Projekt deaktivieren**.

Verwandte Themen

- [Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer SharePoint Online-Umgebung](#) auf Seite 15

Basisdaten für die Verwaltung einer SharePoint Online-Umgebung

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

- Konfigurationsparameter

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

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

Weitere Informationen finden Sie unter [Anhang: Konfigurationsparameter für die Verwaltung einer SharePoint Online-Umgebung](#) auf Seite 52.

- 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 im Zielsystem, wird durch die Zuweisung der Kontendefinition an eine Person über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

Weitere Informationen finden Sie unter [Einrichten von Kontendefinitionen](#) auf Seite 32.

- Zielsystemtypen

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

Weitere Informationen finden Sie unter [Nachbehandlung ausstehender Objekte](#) auf Seite 26.

- Zielsystemverantwortliche

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

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

Weitere Informationen finden Sie unter [Zielsystemverantwortliche](#) auf Seite 49.

Einrichten von Kontendefinitionen

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

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


Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

- [Erstellen einer Kontendefinition](#)
- [Erstellen der Automatisierungsgrade](#)
- [Erstellen einer Abbildungsvorschrift für IT Betriebsdaten](#)
- [Erfassen der IT Betriebsdaten](#)
- [Zuweisen der Kontendefinition an Personen](#)
- [Zuweisen der Kontendefinition an ein Zielsystem](#)

Erstellen einer Kontendefinition

Um eine Kontendefinition zu erstellen

1. Wählen Sie die Kategorie **SharePoint Online | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.

2. Wählen Sie in der Ergebnisliste eine Kontendefinition. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
-ODER-
Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Kontendefinition.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- [Stammdaten einer Kontendefinition](#) auf Seite 33

Verwandte Themen

[Anhang: Verarbeitung von Systemobjekten](#)

Stammdaten einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 10: 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. Wenn die bestellt oder zugeordnet wird, wird die vorausgesetzte automatisch mitbestellt oder zugeordnet. Für SharePoint Online wählen Sie eine Azure Active Directory Kontodefinition aus die Auswahlliste.
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 One Identity Manager Administrationshandbuch für Risikobewertungen.

Eigenschaft	Beschreibung
Leistungsposition	Leistungsposition, über welche die im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.
IT Shop	Angabe, ob die über den IT Shop bestellbar ist. Die kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden.
Verwendung nur im IT Shop	Angabe, ob die ausschließlich über den IT Shop bestellbar ist. Die kann über das Web Portal von den Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der an Rollen außerhalb des IT Shop ist nicht zulässig.
Automatische Zuweisung zu Personen	<p>Angabe, ob die automatisch an alle internen Personen zugewiesen werden soll. Beim Speichern wird die an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine Person neu angelegt wird, erhält sie ebenfalls automatisch diese.</p> <p>Um die automatische Zuweisung der an alle Personen zu entfernen, deaktivieren Sie die Option. Ab diesem Zeitpunkt wird die nicht neu an Personen zugewiesen. Bestehende Zuweisungen der 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	Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Personen.

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

Erstellen der Automatisierungsgrade

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

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

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

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

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

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

Legen Sie für jeden Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll.


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

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

1. Wählen Sie die Kategorie **SharePoint Online | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Automatisierungsgrade zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Automatisierungsgrade zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Automatisierungsgrade.
5. Speichern Sie die Änderungen.

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

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie die Kategorie **SharePoint Online | Basisdaten zur Konfiguration | Kontendefinitionen | Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
-ODER-
Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Automatisierungsgrades.
4. Speichern Sie die Änderungen.

Verwandte Themen

- [Stammdaten eines Automatisierungsgrades](#) auf Seite 37

Stammdaten eines Automatisierungsgrades

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 11: 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: <table border="0" style="margin-left: 20px;"> <tr> <td>Niemals</td> <td>Die Daten werden nicht aktualisiert.</td> </tr> <tr> <td>Immer</td> <td>Die Daten werden immer aktualisiert</td> </tr> <tr> <td>Nur initial</td> <td>Die Daten werden nur initial ermittelt.</td> </tr> </table>	Niemals	Die Daten werden nicht aktualisiert.	Immer	Die Daten werden immer aktualisiert	Nur initial	Die Daten werden nur initial ermittelt.
Niemals	Die Daten werden nicht aktualisiert.						
Immer	Die Daten werden immer aktualisiert						
Nur initial	Die Daten werden nur initial ermittelt.						
Gruppen bei zeitweiliger Deaktivierung beibehalten	Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.						
Benutzerkonten bei zeitweiliger Deaktivierung sperren	Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen gesperrt werden sollen.						
Gruppen bei dauerhafter Deaktivierung beibehalten	Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.						
Benutzerkonten bei dauerhafter Deaktivierung sperren	Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen gesperrt werden sollen.						
Gruppen bei 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.						

Eigenschaft	Beschreibung
Gruppen bei deaktiviertem Benutzerkonto beibehalten	Angabe, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen.

Erstellen einer Abbildungsvorschrift für IT Betriebsdaten

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

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

1. Wählen Sie die Kategorie **SharePoint Online | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **IT Betriebsdaten Mapping bearbeiten** und erfassen Sie folgende Daten.

Tabelle 12: Abbildungsvorschrift für IT Betriebsdaten

Eigenschaft	Beschreibung
Spalte	Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird.
Quelle	<p>Angabe, welche Rolle verwendet wird, um die Eigenschaften für das Benutzerkonto zu ermitteln. Zur Auswahl stehen:</p> <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 <p>Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option Immer Standardwert verwenden setzen.</p>
Standardwert	Standardwert der Eigenschaft für das Benutzerkonto einer

Eigenschaft	Beschreibung
	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.

Verwandte Themen

- [Erfassen der IT Betriebsdaten](#) auf Seite 39

Erfassen der IT Betriebsdaten

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

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

Beispiel:

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

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


Für die Abteilung A legen Sie die wirksamen IT Betriebsdaten für A fest. Diese IT Betriebsdaten werden für die Standardbenutzerkonten verwendet. Zusätzlich legen Sie für

die Abteilung A die wirksamen IT Betriebsdaten für die Kontendefinition B fest. Diese IT Betriebsdaten werden für administrative Benutzerkonten verwendet.

Um IT Betriebsdaten festzulegen

1. Wählen Sie in der Kategorie **Organisationen** bzw. **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten** und erfassen Sie folgende Daten.

Tabelle 13: IT Betriebsdaten

Eigenschaft	Beschreibung
Organisation/Geschäftsrolle	Abteilung, Kostenstelle, Standort oder Geschäftsrolle, für die die IT Betriebsdaten gelten sollen.
Wirksam für	Anwendungsbereich der IT Betriebsdaten. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden. Um den Anwendungsbereich festzulegen <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	Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript TSB_ITDataFromOrg verwenden.
Wert	Konkreter Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.

3. Speichern Sie die Änderungen.

Verwandte Themen

- [Erstellen einer Abbildungsvorschrift für IT Betriebsdaten](#) auf Seite 38

Ändern der IT Betriebsdaten

Sobald sich die IT Betriebsdaten ändern, müssen diese Änderungen für bestehende Benutzerkonten übernommen werden. Dafür müssen die Bildungsregeln an den betroffenen Spalten erneut ausgeführt werden. Bevor die Bildungsregeln ausgeführt werden, können Sie prüfen, 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 Datenbank übernommen werden soll.

Voraussetzungen

- Die IT Betriebsdaten einer Abteilung, Kostenstelle, Geschäftsrolle oder eines Standorts wurden geändert.
- ODER -
- Die Standardwerte in der IT Betriebsdaten Abbildungsvorschrift für eine Kontendefinition wurden geändert.

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

Um die Bildungsregeln auszuführen

1. Wählen Sie 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.

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

Detaillierte Informationen zum Thema

- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 43
- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 43
- [Kontendefinition an alle Personen zuweisen](#) auf Seite 44
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 45
- [Zuweisen der Kontendefinition an ein Zielsystem](#) auf Seite 47

Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie 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.

- ODER -

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

Verwandte Themen

- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 43
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 45

Kontendefinition an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie 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.
 - ODER -

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

Verwandte Themen

- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 43
- [Kontendefinition an alle Personen zuweisen](#) auf Seite 44
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 45

Kontendefinition an alle Personen zuweisen

Um eine Kontendefinition an alle Personen zuzuweisen

1. Wählen Sie 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.

Verwandte Themen

- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 43
- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 43
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 45

Kontendefinition direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

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

Verwandte Themen

- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 43
- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 43
- [Kontendefinition an alle Personen zuweisen](#) auf Seite 44

Kontendefinition an Systemrollen zuweisen

Installierte Module: Systemrollenmodul

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

Um Kontendefinitionen in eine Systemrolle aufzunehmen

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

Kontendefinition in den IT Shop aufnehmen

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

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

1 **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 in der Ergebnisliste die Kontendefinition.
2. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontendefinition an die IT Shop Regale zu.
4. Speichern Sie die Änderungen.

Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie in der Ergebnisliste die Kontendefinition.
2. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
3. Entfernen Sie im Bereich **Zuordnungen entfernen** die Kontendefinition aus den IT Shop Regalen.
4. Speichern Sie die Änderungen.

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie in der Ergebnisliste die Kontendefinition.
2. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
3. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
4. Klicken Sie **OK**.

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

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

Verwandte Themen

- [Stammdaten einer Kontendefinition](#) auf Seite 33
- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 43
- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 43
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 45
- [Kontendefinition an Systemrollen zuweisen](#) auf Seite 45

Zuweisen der Kontendefinition an ein Zielsystem

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

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

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

Um die Kontendefinition an ein Zielsystem zuzuweisen

1. Wählen Sie 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

- [Zuweisen der Kontendefinition an Personen](#) auf Seite 42

Löschen einer Kontendefinition


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

- ① **HINWEIS:** Wird eine Kontendefinition gelöscht, dann werden die Benutzerkonten, die aus dieser Kontendefinition entstanden sind, gelöscht.

Um eine Kontendefinition zu löschen

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Personen.
 - a. Wählen Sie 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 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 Standorte.
 - a. Wählen Sie 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 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. Wenn die Kontendefinition über den IT Shop bestellt wurde, muss sie abbestellt und aus allen IT Shop Regalen entfernt werden. Ausführliche Informationen dazu finden Sie im One Identity Manager Administrationshandbuch für IT Shop.
6. Entfernen Sie die Zuordnung der Kontendefinition als vorausgesetzte Kontendefinition einer anderen Kontendefinition. Solange die Kontendefinition Voraussetzung einer anderen Kontendefinition ist, kann sie nicht gelöscht werden.

Prüfen Sie alle Kontendefinitionen.

- a. Wählen Sie 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.
7. Entfernen Sie die Zuordnung der Kontendefinition zum Zielsystem.
- a. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
 - b. Entfernen Sie auf dem Tabreiter **Allgemein** die zugewiesenen Kontendefinitionen.
 - c. Speichern Sie die Änderungen.
8. Löschen Sie die Kontendefinition.
- a. Wählen Sie 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.

Zielsystemverantwortliche

Ausführliche Informationen zum Einsatz und zur Bearbeitung von Anwendungsrollen finden Sie im One Identity Manager Administrationshandbuch für Anwendungsrollen.

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

1. Der One Identity Manager Administrator legt Personen als Zielsystemadministratoren fest.
2. Die Zielsystemadministratoren nehmen die Personen in die Standardanwendungsrolle für die Zielsystemverantwortlichen auf.
Zielsystemverantwortliche der Standardanwendungsrolle sind berechtigt alle SharePoint Online Websitesammlungen 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 14: 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 zur Aufnahme in den IT Shop vor.• 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 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.

- Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Zielsysteme | SharePoint Online** zu.
 - 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 6

Anhang: Konfigurationsparameter für die Verwaltung einer SharePoint Online-Umgebung

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

Tabelle 15: Konfigurationsparameter für die Verwaltung einer SharePoint Online-Umgebung

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	Der Konfigurationsparameter erlaubt die Konfiguration der Angaben zu Empfängern.
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.

Konfigurationsparameter	Bedeutung
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.
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.

Anhang: 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.

Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 16: Abbildung der SharePoint Online Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im SharePoint Online	Tabelle im One Identity Manager Schema
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.

Anhang: 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 17: 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 besuchen Sie <https://www.oneidentity.com/company/contact-us.aspx> oder rufen Sie + 1-800-306-9329 an.

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 5
- Ausstehendes Objekt 26
- Azure Active Directory Mandant
 - Kontendefinition (initial) 47

B

- Benutzerkonto
 - Bildungsregeln ausführen 41
- Bildungsregel
 - IT Betriebsdaten ändern 41

I

- IT Betriebsdaten
 - ändern 41
- IT Shop Regal
 - Kontendefinitionen zuweisen 46

J

- Jobserver
 - bearbeiten 12

K

- Konfigurationsparameter 52
- Kontendefinition 32
 - an Abteilung zuweisen 43
 - an alle Personen zuweisen 44
 - an Azure Active Directory Mandanten zuweisen 47
 - an Geschäftsrolle zuweisen 43

- an Kostenstelle zuweisen 43
- an Person zuweisen 42, 45
- an Standort zuweisen 43
- an Systemrollen zuweisen 45
- automatisch zuweisen 44
- Automatisierungsgrad 35
- erstellen 32
- in IT Shop aufnehmen 46
- IT Betriebsdaten 38-39
- löschen 47

M

- Mitgliedschaft
 - Änderung provisionieren 28

O

- Objekt
 - ausstehend 26
 - publizieren 26
 - sofort löschen 26

P

- Projektvorlage 54
- Provisionierung
 - Mitgliederliste 28

S

- Schema
 - aktualisieren 25

- Änderungen 25
 - komprimieren 25
- SharePoint Online Konnektor 5
- SharePoint Online Organisation
 - Zielsystemverantwortlicher 49
- SharePoint Online Server 5
- Synchronisation
 - konfigurieren 15, 23
 - Scope 23
 - starten 15
 - Synchronisationsprojekt
 - erstellen 15
 - Variable 23
 - Verbindungsparameter 15, 23
 - verhindern 30
 - Workflow 15, 24
- Synchronisationsanalysebericht 29
- Synchronisationskonfiguration
 - anpassen 23-24
- Synchronisationsprojekt
 - deaktivieren 30
 - erstellen 15
 - Projektvorlage 54
- Synchronisationsprotokoll 21
- Synchronisationsrichtung
 - In das Zielsystem 15, 24
 - In den Manager 15
- Synchronisationsserver 5
 - installieren 12
 - Jobserver 12
 - konfigurieren 12
- Synchronisationsworkflow
 - erstellen 15, 24

Z

- Zeitplan
 - deaktivieren 30
- Zielsystemabgleich 26
- Zielsystemverantwortlicher 49