One Identity Manager 8.1.4

Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung

Legende

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

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

One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung
Aktualisiert - 19. Oktober 2020, 08:24 Uhr
Version - 8.1.4

Inhalt

Verwalten einer Exchange Online-Umgebung

Die Schwerpunkte der Verwaltung einer Exchange Online-Umgebung mit dem One Identity Manager liegen in der Abbildung von Postfächern, E-Mail Benutzern, E-Mail Kontakten, E-Mail aktivierten Verteilergruppen und Office 365- Gruppen die in einer Cloud-Umgebung liegen.

Durch die Datensynchronisation werden die Systeminformationen zur Exchange 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 Exchange Online Struktur finden Sie in der Exchange Online Dokumentation von Microsoft.

Verwandte Themen

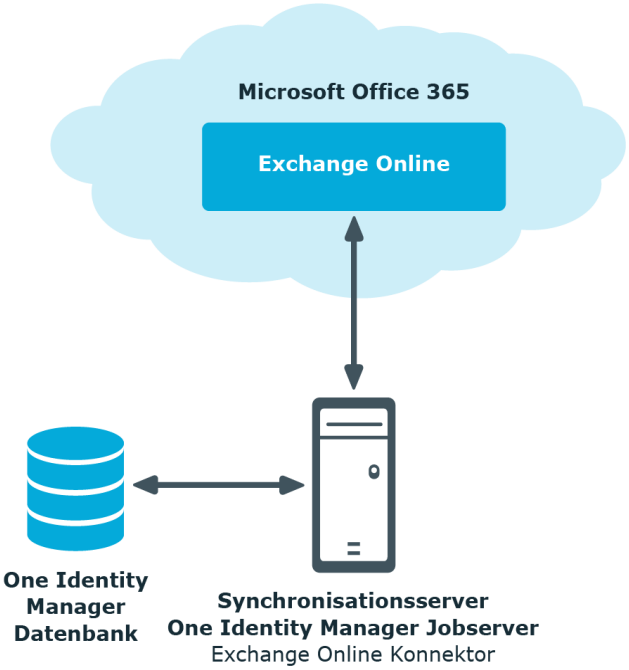
- Verarbeitung von Systemobjekten

Architekturüberblick

Um auf die Daten einer Exchange Online-Organisation zuzugreifen, wird auf einem Synchronisationsserver der Exchange Online Konnektor installiert. Der Synchronisationsserver sorgt für den Abgleich der Daten zwischen der One Identity Manager-Datenbank und Exchange Online. Der Exchange Online Konnektor ist Bestandteil des Exchange Online Moduls und verantwortlich für die Kommunikation mit den Microsoft Office 365 Abonnements des Exchange Online in der Cloud. Windows PowerShell wird für den Zugriff auf die Exchange Online Daten verwendet.

Für den Zugriff auf die Daten einer Exchange 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 Exchange Online-Umgebung

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

Tabelle 1: Benutzer

Benutzer	Aufgaben
Zielsystemadministratoren	Die Zielsystemadministratoren müssen der Anwendungsrolle **Zielsysteme | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen. • Legen die Zielsystemverantwortlichen fest. • Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein.

Benutzer	Aufgaben
	• Legen fest, welche Anwendungsrollen für Zielsystemverantwortliche sich ausschließen. • Berechtigen weitere Personen als Zielsystemadministratoren. • Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Exchange Online** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.
One Identity Manager Administratoren	• Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse.

Benutzer	Aufgaben
	• Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.

Einrichten der Synchronisation mit einer Exchange Online-Umgebung

Der One Identity Manager unterstützt die Synchronisation mit Exchange Online.

Für den Abgleich der Informationen zwischen der One Identity Manager-Datenbank und der Exchange 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.

Um die Objekte einer Exchange 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 Exchange Online-Umgebungen sind verfügbar, wenn der Konfigurationsparameter **TargetSystem | AzureAD | ExchangeOnline** 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 Exchange Online-Umgebung auf Seite 10
- Einrichten des Synchronisationsservers auf Seite 12

- Konfiguration der beteiligten Server für den Remotezugriff über Windows PowerShell auf Seite 16
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Exchange Online-Umgebung auf Seite 17
- Deaktivieren der Synchronisation auf Seite 37
- Besonderheiten zur Synchronisation von Exchange Online-Umgebungen auf Seite 26
- Anpassen einer Synchronisationskonfiguration auf Seite 28
- Konfigurationsparameter für die Verwaltung einer Exchange Online-Umgebung auf Seite 62
- Standardprojektvorlagen für Exchange Online auf Seite 64

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

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

Tabelle 2: Benutzer für die Synchronisation

Benutzer	Berechtigungen
Benutzer für den Zugriff auf Exchange Online	Für eine vollständige Synchronisation von Objekten einer Exchange Online-Umgebung mit der ausgelieferten One Identity Manager Standardkonfiguration stellen Sie ein Benutzerkonto bereit, das die folgenden Berechtigungen besitzt. • Mitglied in der Rollengruppe "Organisationsverwaltung" (Organization Management) • Mitglied in der Rollengruppe "Empfängerverwaltung" (Recipient Management) HINWEIS: Beachten Sie die Kennwortlaufzeit für das Benutzerkonto für die Synchronisation. Abgelaufene Kennworte verursachen Synchronisationsfehler. Sie können die Kennwortablaufzeit des Benutzerkontos in One Identity Manager deaktivieren. Weitere Informationen finden Sie im One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung.
Benutzerkonto des One Identity Manager Service	Das Benutzerkonto für den One Identity Manager Service benötigt die Rechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Rechte vergeben, Verzeichnisse und Dateien anlegen

Benutzer	Berechtigungen
	und bearbeiten. Das Benutzerkonto muss der Gruppe **Domänen-Benutzer** angehören. Das Benutzerkonto benötigt das erweiterte Benutzerrecht **Anmelden als Dienst**. Das Benutzerkonto benötigt Rechte für den internen Webservice. HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so können Sie die Rechte für den internen Webservice über folgenden Kommandozeilenaufruf vergeben: `netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"` Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis. In der Standardinstallation wird der One Identity Manager installiert unter: • `%ProgramFiles(x86)%\One Identity` (auf 32-Bit 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 Rollen in den das Benutzerkonto für die Synchronisation Mitglied werden soll sind:

- Organisationsverwaltung
  Administratoren, die Mitglieder der Rollengruppe Organisationsverwaltung sind, verfügen über Administratorzugriff auf die gesamte Exchange Online-Organisation und können praktisch sämtliche Aufgaben für ein beliebiges Exchange Online-Objekt ausführen. Es gelten jedoch einige Ausnahmen (zum Beispiel: die Rolle Discovery Management).
- Empfängerverwaltung
  Administratoren, die Mitglied der Rollengruppe Empfängerverwaltung sind, haben Administratorzugriff zum Erstellen oder Ändern von Exchange Online-Empfängern innerhalb der Exchange Online-Organisation.

Nachfolgend werden zwei Varianten beschrieben wie Sie diese Berechtigungen zuweisen können.

Um Berechtigungen über das Microsoft Online Portal zuzuweisen

HINWEIS: Um diese Variante zu nützen muss eine Lizenz an das Benutzerkonto für die Synchronisation zugewiesen werden.

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 Admin center Portal zu öffnen.
3. Wählen Sie aus dem Menü auf der linken Seite, **Admin Center | Exchange**.
   Damit wechseln Sie zum Exchange Admin Center.
4. Klicken Sie auf **Berechtigungen** im Menü auf der linken Seite.
5. Wählen Sie **Recipient Management** und klicken das Bearbeitungssymbol in der Symbolleiste.
6. Fügen Sie das Benutzerkonto für die Synchronisation unter **Mitglieder** ein.
7. Wiederholen Sie die Schritte 5 und 6 für die Rolle **Organisationsverwaltung**.

HINWEIS: Für den Fall, dass Sie das Benutzerkonto für die Synchronisation nicht in der Liste der Mitglieder finden, können Sie die Berechtigungen über Windows PowerShell erteilen. Möglicherweise besitzt das Benutzerkonto kein Postfach oder keine zugewiesene Office 365 Lizenz. In diesem Fall nutzen Sie die nächste Variante.

Einrichten des Synchronisationsservers

Für die Einrichtung der Synchronisation mit einer Exchange 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 4.7.2 oder höher

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.
- Windows Management Framework 4.0
- One Identity Manager Service, Exchange 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 | Exchange Online**.

WICHTIG: Der Exchange Online Konnektor des One Identity Manager verwendet Windows PowerShell für die Kommunikation mit dem Microsoft Exchange Server. Für die Kommunikation sind zusätzliche Konfigurationen auf dem Synchronisationsserver und im Exchange Online vorzunehmen. Weitere Informationen finden Sie unter Konfiguration der beteiligten Server für den Remotezugriff über Windows PowerShell auf Seite 16.

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 folgende Schritte aus:

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

HINWEIS: Für die Generierung von Prozessen für die Jobserver werden der Provider, Verbindungsparameter und die Authentifizierungsdaten benötigt. Diese Informationen werden im Standardfall aus den Verbindungsdaten der Datenbank ermittelt. Arbeitet der Jobserver über einen Anwendungsserver müssen Sie zusätzliche Verbindungsinformationen im Designer konfigurieren. Ausführliche Informationen zum Einrichten des Jobservers finden Sie im *One Identity Manager Konfigurationshandbuch*.

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

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

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

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

      - ODER -

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

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

        Syntax:

        `<Name des Servers>.<Vollqualifizierter Domänenname>`

   HINWEIS: Über die Option **Erweitert** können Sie weitere Eigenschaften für den Jobserver bearbeiten. Sie können die Eigenschaften auch zu einem späteren Zeitpunkt mit dem Designer bearbeiten.
4. Auf der Seite **Maschinenrollen** wählen Sie **Exchange Online**.
5. Auf der Seite **Serverfunktionen** wählen Sie **Exchange Online Konnektor (via Windows PowerShell)**.
6. Auf der Seite **Dienstkonfiguration** erfassen Sie die Verbindungsinformationen und prüfen Sie die Konfiguration des One Identity Manager Service.

   HINWEIS: Die initiale Konfiguration des Dienstes ist bereits vordefiniert. Sollte eine erweiterte Konfiguration erforderlich sein, können Sie diese auch zu einem späteren Zeitpunkt mit dem Designer durchführen. Ausführliche Informationen zur Konfiguration des Dienstes finden Sie im *One Identity Manager Konfigurationshandbuch*.

   - Für eine direkte Verbindung zu Datenbank:
     a. Wählen Sie **Prozessabholung | sqlprovider**
     b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     c. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.

- Für eine Verbindung zum Anwendungsserver:
    a. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
    b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
    c. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.
    d. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
    e. Wählen Sie das Authentifizierungsmodul. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

7. Zur Konfiguration der Remote-Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** wählen Sie das Verzeichnis mit den Installationsdateien.
10. Auf der Seite **Datenbankschlüsseldatei auswählen** wählen die Datei mit dem privaten Schlüssel.

    HINWEIS: Diese Seite wird nur angezeigt, wenn die Datenbank verschlüsselt ist.
11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
    - **Computer**: Name oder IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
    - **Dienstkonto**: Angaben zum Benutzerkonto des One Identity Manager Service.
        - Um den Dienst unter dem Konto **NT AUTHORITY\SYSTEM** zu starten, aktivieren Sie die Option **Lokales Systemkonto**.
        - Um den Dienst unter einem anderen Konto zu starten, deaktivieren Sie die Option **Lokales Systemkonto** und erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung.
    - **Installationskonto**: Angaben zum administrativen Benutzerkonto für die Installation des Dienstes.
        - Um das Benutzerkonto des angemeldeten Benutzers zu verwenden, aktivieren Sie die Option **Angemeldeter Benutzer**.
        - Um ein anderes Benutzerkonto zu verwenden, deaktivieren Sie die Option **Angemeldeter Benutzer** und geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.
    - Um das Installationsverzeichnis, den Namen, den Anzeigenamen oder die Beschreibung für den One Identity Manager Service zu ändern, nutzen Sie die weiteren Optionen.

12. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.

    Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.

13. Auf der letzten Seite des Server Installer klicken Sie **Fertig**.

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

Verwandte Themen

- Konfiguration der beteiligten Server für den Remotezugriff über Windows PowerShell auf Seite 16

Konfiguration der beteiligten Server für den Remotezugriff über Windows PowerShell

HINWEIS: Führen Sie die Konfigurationsschritte auf dem Synchronisationsserver aus.

Um einen Server für den Remotezugriff über Windows PowerShell zu konfigurieren

1. Führen Sie eine Windows PowerShell über das Kontextmenü **Als Administrator ausführen** mit administrativen Rechten aus.
2. Geben Sie in der Eingabeaufforderung den Befehl ein:

   ```
   winrm quickconfig
   ```

   Mit diesem Befehl wird die Nutzung des Remotezugriffs vorbereitet.
3. Geben Sie in der Eingabeaufforderung den Befehl ein:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

   Mit diesem Befehl wird die Ausführung von Windows PowerShell-Befehle (Cmdlets) zugelassen. Die Skripte müssen von einem vertrauenswürdigen Herausgeber signiert sein.

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

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

HINWEIS: Beachten Sie bei der Einrichtung der Synchronisation die unter Besonderheiten zur Synchronisation von Exchange Online-Umgebungen auf Seite 26 beschriebenen Empfehlungen.

WICHTIG: Erstellen Sie für jede Exchange Online-Umgebung ein eigenes Synchronisationsprojekt.

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.

WICHTIG: Für eine erfolgreiche Authentifizierung muss Exchange Online per DNS Anfrage erreicht werden können. Ist die DNS Auflösung nicht möglich, wird die Verbindung zum Zielsystem mit Fehlermeldung abgelehnt.

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.

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

Tabelle 3: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen

Benutzername und Kennwort zur Anmeldung	Benutzerkonto und Kennwort zur Authentifizierung am Exchange Online.
	Beispiel:
	`<user>@<domain.com>`
	`<Benutzername des Synchronisationsnutzers>@yourorganisation.onmicrosoft.com`
	Stellen Sie ein Benutzerkonto mit ausreichend

<table>
<tr><th>Angaben</th><th>Erläuterungen</th></tr>
<tr><td></td><td>Berechtigungen bereit. Weitere Informationen finden Sie unter Benutzer und Berechtigungen für die Synchronisation mit einer Exchange Online-Umgebung auf Seite 10.</td></tr>
<tr><td>Synchronisationsserver für Exchange Online</td><td>Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem Exchange Online Konnektor installiert sein.

Tabelle 4: Zusätzliche Eigenschaften für den Jobserver<table><tr><th>Eigenschaft</th><th>Wert</th></tr><tr><td>Serverfunktion</td><td>Exchange Online Konnektor</td></tr><tr><td>Maschinenrolle</td><td>Server/Jobserver/Azure Active Directory/ExchangeOnline</td></tr></table>
Weitere Informationen finden Sie unter Einrichten des Synchronisationsservers auf Seite 12.</td></tr>
<tr><td>Verbindungsdaten zur One Identity Manager-Datenbank</td><td>Datenbankserver
Datenbank
SQL Server Anmeldung und Kennwort
Angabe, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.</td></tr>
<tr><td>Remoteverbindungsserver</td><td>Um die Synchronisation mit einem Zielsystem zu konfigurieren, muss der One Identity Manager Daten aus dem Zielsystem auslesen. Dabei kommuniziert der One Identity Manager direkt mit dem Zielsystem. Mitunter ist der direkte Zugriff von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, nicht möglich, beispielsweise aufgrund der Firewall-Konfiguration oder weil die Arbeitsstation nicht die notwendigen Hard- oder Softwarevoraussetzungen erfüllt. Wenn der direkte Zugriff von der Arbeitsstation nicht möglich ist, kann eine Remoteverbindung eingerichtet werden.

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

Konfiguration des Remoteverbindungsservers:</td></tr>
</table>

Angaben	Erläuterungen
	• One Identity Manager Service ist gestartet • **RemoteConnectPlugin** ist installiert • Exchange Online Konnektor ist installiert Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt. TIPP: Der Remoteverbindungsserver benötigt dieselbe Konfiguration (bezüglich der installierten Software sowie der Berechtigungen des Benutzerkontos) wie der Synchronisationsserver. Nutzen Sie den Synchronisationsserver gleichzeitig als Remoteverbindungsserver, indem Sie lediglich das `RemoteConnectPlugin` zusätzlich installieren. Ausführliche Informationen zum Herstellen einer Remoteverbindung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

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 Exchange Online-Umgebung einzurichten

1. Starten Sie das Launchpadund 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 Exchange Online** und klicken Sie **Starten**.

   Der Projektassistent des Synchronization Editors wird gestartet.

3. Auf der Seite **Systemzugriff** legen Sie fest, wie der One Identity Manager auf das Zielsystem zugreifen kann.
   - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, möglich, nehmen Sie keine Einstellungen vor.
   - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor

gestartet haben, nicht möglich, können Sie eine Remoteverbindung herstellen.

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

4. Auf der Seite **Verbindungsparameter** erfassen Sie die Anmeldeinformationen für die Verbindung zum Exchange Online.

Tabelle 5: Verbindungsparameter zum Exchange Online

Eigenschaft	Beschreibung

Benutzername (user@-domain)	Vollqualifizierter Name (FQDN) des Benutzerkonto zur Anmeldung.
	Beispiel:
	`<user>@<domain.com>`
	`sync.user@yourorganisation.onmicrosoft.com`

Kennwort	Kennwort zum Benutzerkonto.

Mit **Satz hinzufügen** können Sie weitere Verbindungsparameter eingeben. Damit legen Sie mehrere Synchronisationsbenutzer an. Diese werden vom Exchange Online Konnektor zyklisch abgefragt, wenn Anfragen an Exchange Online gesendet werden. Durch die Verwendung mehrere Synchronisationsbenutzer wird der Einschränkungsgrenzwert langsamer erreicht.

Ausführliche Information zur Einschränkungsgrenzwerte in Exchange Online finden Sie in der Exchange Online Dokumentation von Microsoft.

Um die Verbindungsparameter einzeln zu testen, klicken Sie ☑ innerhalb des Satzes. Klicken Sie **Alle Sätze prüfen** um alle Sätze auf einmal zu prüfen.

Klicken Sie **Weiter**.

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

Tabelle 6: 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

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

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

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

   a. Klicken Sie , um einen neuen Jobserver anzulegen.

   b. Erfassen Sie die Bezeichnung des Jobservers und den vollständigen Servernamen gemäß DNS-Syntax.

   c. Klicken Sie **OK**.

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

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

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

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

   Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

   HINWEIS: Beim Aktivieren wird eine Konsistenzprüfung durchgeführt. Wenn dabei

Fehler auftreten, erscheint eine Meldung. Sie können entscheiden, ob das Synchronisationsprojekt dennoch aktiviert werden soll.

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

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

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

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

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

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

Um regelmäßige Synchronisationen auszuführen

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

Um die initiale Synchronisation manuell zu starten

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

Ausführen.

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

Verwandte Themen

- Einrichten des Synchronisationsservers auf Seite 12
- Erweiterte Einstellungen für den Exchange Online Konnektor
- Benutzer und Berechtigungen für die Synchronisation mit einer Exchange Online-Umgebung auf Seite 10
- Synchronisationsergebnisse anzeigen auf Seite 25
- Besonderheiten zur Synchronisation von Exchange Online-Umgebungen auf Seite 26
- Anpassen einer Synchronisationskonfiguration auf Seite 28
- Standardprojektvorlagen für Exchange Online auf Seite 64

Erweiterte Einstellungen für den Exchange Online Konnektor

Im Projektassistenten des Synchronization Editors können Sie auf der Seite **Verbindungen zu Exchange Online** festlegen, ob Sie erweiterte Einstellungen benötigen. Diese Einstellungen erlauben Ihnen folgende Optionen der Kommunikation mit Exchange Online zu ändern:

- die Anzahl der gleichzeitigen Verbindungen pro Verbindungsparametersatz
- die Definition der Windows PowerShell Befehle

Anzahl der gleichzeitigen Verbindungen pro Verbindungsparametersatz

> WICHTIG: Diese Option sollte nur mit Anweisungen eines Support-Mitarbeiters geändert werden. Änderungen an dieser Einstellung haben weitreichende Auswirkungen in der Synchronisation und müssen deshalb sehr vorsichtig behandelt werden.

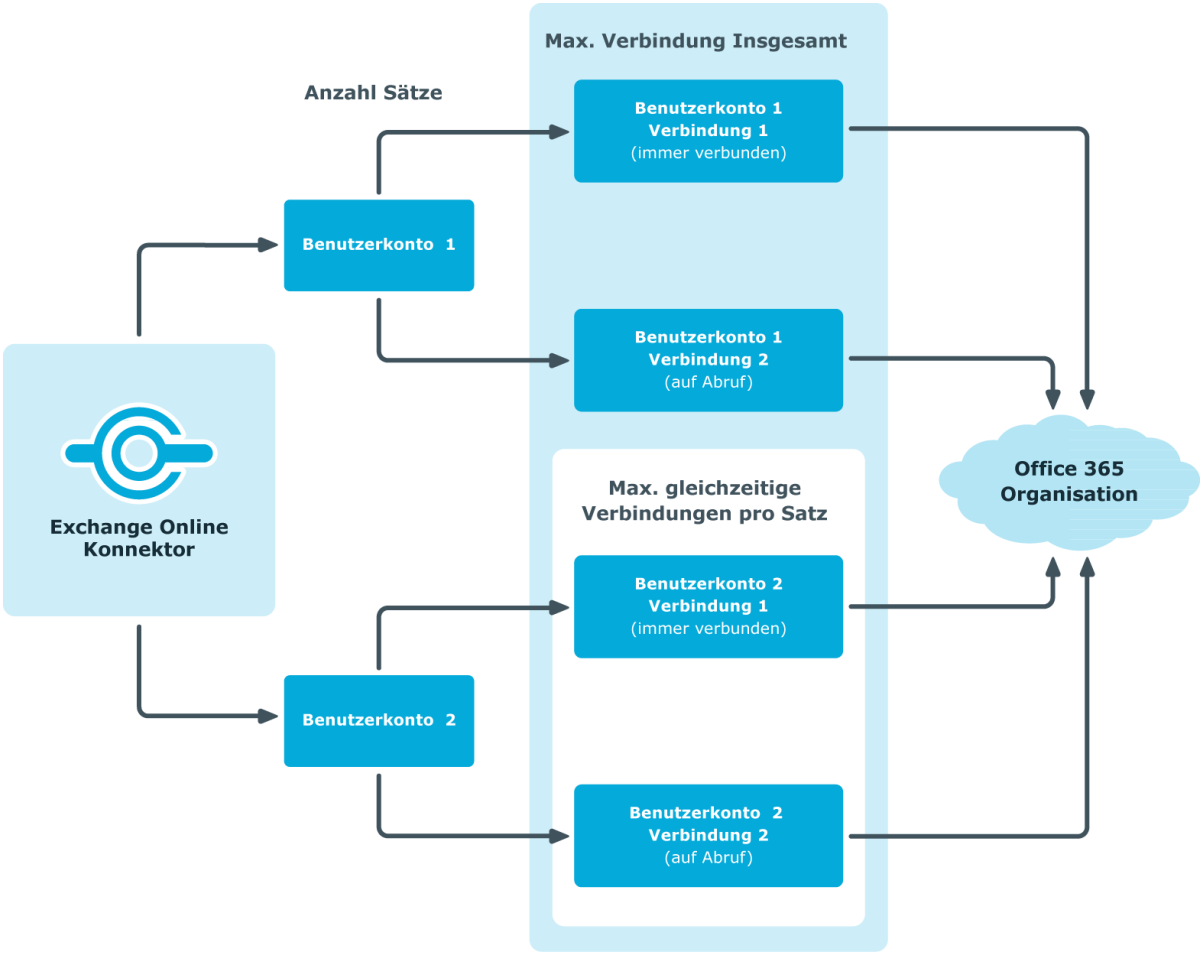
Mit dieser Option können Sie die Anzahl der gleichzeitigen Verbindungen pro Verbindungsparametersatz beziehungsweise pro Benutzerkonto für die Synchronisation festlegen. Die Einstellung legt fest, wie viele gleichzeitige Verbindungen pro Benutzerkonto erstellt werden können. Der Standardwert ist 2. Serverseitig lässt Exchange Online aktuell 3 Verbindungen pro Benutzer zu.

Wenn sich der Exchange Online Konnektor verbindet, erstellt er eine Windows PowerShell Sitzung pro Verbindungsparametersatz unabhängig von der Anzahl der anschließenden Anfragen. Weitere Verbindungen werden dynamisch hinzugefügt falls sie benötigt werden, zum Beispiel, beim Laden mehrerer Objekte während der Synchronisation.

Die maximale Anzahl der Sitzungen, die gegen Exchange Online erstellt werden können, können Sie mit folgender Formel berechnen:

`Maximale Anzahl Windows PowerShell Sitzungen = Anzahl Verbindungsparametersätze * Wert in Anzahl der gleichzeitiger Verbindungen pro Verbindungsparametersatz`

Die minimale Anzahl der Sitzungen, die gegen Exchange Online erstellt werden können, ist gleich der Anzahl der Verbindungsparametersätze.



Um die Anzahl der gleichzeitigen Verbindungen zu ändern

1. Auf der Seite **Verbindung zu Exchange Online** im Verbindungsassistent des Synchronization Editors wählen Sie die Option **Erweiterte Einstellungen anzeigen** und klicken Sie **Weiter**.
2. Geben Sie einen Wert zwischen 1 und 3 im **Eingabefeld gleichzeitige Verbindungen pro Verbindungsparametersatz** ein.
3. Auf der Seite **Verbindungsparameter** erfassen Sie die Anmeldeinformationen für die Verbindung zum Exchange Online. Weitere Informationen finden Sie unter Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Exchange Online-Umgebung
4. Klicken Sie **Fertig** zum beenden.

Anpassen der Konnektordefinition

Mit dieser Einstellung können Sie die Definition anpassen, die vom Konnektor verwendet wird, um Ein- und Ausgaben zwischen den Exchange Online Cmdlets und dem Schema der Synchronization Engine umzusetzen.

WICHTIG: Die Konnektordefinition sollte nur mit Anweisungen eines Support-Mitarbeiters geändert werden. Änderungen an dieser Einstellung haben weitreichende Auswirkungen in der Synchronisation und müssen deshalb sehr vorsichtig behandelt werden.

HINWEIS: Eine angepasste Konnektordefinition wird nicht standardmäßig überschrieben, wenn eine neue Version des Konnektors beziehungsweise eine aktualisierte Konnektordefinition herausgegeben wird.

Um die Konnektordefinition anzupassen

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

   Der Systemverbindungsassistent wird gestartet.
4. Auf der Startseite des Systemverbindungsassistenten aktivieren Sie **Erweiterte Einstellungen anzeigen**.
5. Auf der Seite **Erweiterte Einstellungen** passen Sie die Konnektordefinition an.
   a. Wählen Sie die Option **Konnektordefinition anpassen**.
   b. Bearbeiten Sie die Definition in Absprache mit dem Support-Mitarbeiter. Sie können folgende Aktionen ausführen:
      - Mit laden Sie die Definition aus einer Datei.
      - Mit prüfen Sie die Definition auf Fehler.
      - Mit zeigen Sie die Unterschiede zur Standardversion an.
6. Speichern Sie die Änderungen.

Synchronisationsergebnisse anzeigen

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

Um das Protokoll einer Synchronisation anzuzeigen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Protokolle**.

3. Klicken Sie in der Symbolleiste der Navigationsansicht ▶.

   In der Navigationsansicht werden die Protokolle aller abgeschlossenen Synchronisationsläufe angezeigt.

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

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

Um das Protokoll einer Provisionierung anzuzeigen

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

   In der Navigationsansicht werden die Protokolle aller abgeschlossenen Provisionierungsprozesse angezeigt.

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

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

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

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

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

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

Besonderheiten zur Synchronisation von Exchange Online-Umgebungen

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

Abhängigkeitsauflösung

Automatische Synchronisationsschritt Abhängigkeitsauflösung ist im Synchronisationsworkflow standardmäßig ausgeschaltet. Damit wird die Anzahl der benötigten Anfragen an Exchange Online reduziert. Dies kann aber zu nicht auflösbaren Referenzen während der Synchronisation führen, die in der Wartungsphase am Ende der Synchronisation bearbeitet werden.

Mehrfache Organisationen nicht unterstützt

Parametersätze können nicht zur Parametrisierung der Verbindung benutzt werden, weil die Anzahl der benutzten Benutzerkonten für die Synchronisation nicht immer gleich ist. Deshalb wird die Erstellung weiterer Basisobjekte innerhalb eines Synchronisationsprojekts nicht unterstützt.

Ändern der Postfachtypen im Exchange Online Portal

Die Standardvorlage für Exchange Online unterstützt die Konvertierung Postfachtypen wie folgt:

- Freigegebenes Postfach in Benutzerpostfach
- Benutzerpostfach in freigegebenes Postfach
- Gerätepostfach in Raumpostfach
- Raumpostfach in Gerätepostfach

HINWEIS: Wenn Sie eine nicht unterstützte Konvertierung vornehmen, zum Beispiel ein Raumpostfach in ein freigegebenes Postfach umwandeln, wird das Raumpostfach als 'Fehlt' von der Synchronisation markiert und das freigegebenes Postfach wird wegen einer Namensverletzung nicht erstellt. Dieses Szenario kann nur mit manuellen Auflösung gelöst werden.

HINWEIS: One Identity Manager unterstützt die Bearbeitung des Postfachtyps nicht.

Statistikdaten über Postfachnutzung synchronisieren

Die Statistikdaten über Postfachnutzung werden in einem eigenen Synchronisationsschritt getrennt synchronisiert. Die Daten aus Exchange Online zu lesen kann gegebenenfalls viel Zeit in Anspruch nehmen. Deshalb bietet es sich an einen separaten Workflow zu erstellen, der einen Synchronisationsschritt zum Lesen die Daten beinhaltet. Sie können das Ausführungsintervall für diesen Workflow in längeren Abständen konfigurieren als den Workflow ohne Nutzungsinformationen.

Folgende Nutzungsdaten werden synchronisiert:

Schemaeigenschaft im Zielsystem	Beschreibung
AssociatedItemCount	Anzahl zugeordneter Elemente in diesem Postfach.
DeletedItemCount	Anzahl der gelöschten Elemente.
DumpsterMessagesPerFolderCountReceiveQuota	Maximale Anzahl an Nachrichten, die ein Ordner im Ordner "Wieder-herstellbare Elemente" enthalten darf.
DumpsterMessagesPerFolderCountWarningQuota	Anzahl der Elemente, die ein Ordner im Ordner "Wiederherstellbare Elemente" enthalten darf, bevor der Benutzer eine Warnung erhält.

Schemaeigenschaft im Zielsystem	Beschreibung
ItemCount	Anzahl der Nachrichten in diesem Postfach (zum Beispiel E-Mail, Kalender, Kontakte) die für die Benutzer sichtbar sind.
LastLoggedOnUserAccount	Name des letzten angemeldeten Benutzers.
LastLogOffTime	Uhrzeit der letzten Abmeldung.
LastLogonTime	Zeitpunkt der letzten Anmeldung.
StorageLimitStatus	Kennzeichnet den Füllstand des Postfachs gegenüber den festgelegten Grenzwerten.
TotalDeletedItemSize	Größe der Elemente im Ordner "Wiederherstellbare Elemente".
TotalItemSize	Vom Postfach belegter Speicher in KB.

HINWEIS: Die Postfachnutzungsinformationen sind nur für Benutzer beziehungsweise freigegebene Postfächer verfügbar.

Anzahl externer Slots für die Jobserver Konfiguration

Da die Anzahl gleichzeitiger Verbindungen in Exchange Online auf 3 pro Benutzer begrenzt ist, wird empfohlen einen dedizierten Jobserver mit maximal 2 externe Slots zu benutzen. Wenn zu viele Verbindungen aktiv sind, wird eine Fehlermeldung angezeigt.

Sie können die Anzahl von Verbindungen pro Verbindungsparametersatz festlegen und die Konnektordefinition anpassen. Weitere Informationen finden Sie unter Erweiterte Einstellungen für den Exchange Online Konnektor auf Seite 23.

Anpassen einer Synchronisationskonfiguration

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation einer Exchange Online-Umgebung eingerichtet. Mit diesem Synchronisationsprojekt können Sie Exchange Online Objekte in die One Identity Manager-Datenbank einlesen. Wenn Sie Postfächer, E-Mail Benutzer, E-Mail Kontakte, E-Mail aktivierte Verteilergruppen und Office 365-Gruppen mit dem One Identity Manager verwalten, werden Änderungen in die Exchange Online-Umgebung provisioniert.

Um die One Identity Manager-Datenbank und die Exchange 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 Exchange 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 Zielsystemschema geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.

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

- Wenn eine weitere Synchronisation mit derselben Startkonfiguration gestartet wird, wird dieser Prozess gestoppt und erhält den Ausführungsstatus **Frozen**. Es wird eine Fehlermeldung in die Protokolldatei des One Identity Manager Service geschrieben.
    - Stellen Sie sicher, dass Startkonfigurationen, die in Startfolgen verwendet werden, nicht gleichzeitig einzeln gestartet werden. Weisen Sie den Startfolgen und Startkonfigurationen unterschiedliche Zeitpläne zu.
- Wenn eine weitere Synchronisation mit einer anderen Startkonfiguration gestartet wird, die dasselbe Zielsystem anspricht, kann das zu Synchronisationsfehlern oder Datenverlust führen. Legen Sie an den Startkonfigurationen fest, wie sich der One Identity Manager in diesem Fall verhalten soll.
    - Stellen Sie über den Zeitplan sicher, dass die Startkonfigurationen nacheinander ausgeführt werden.
    - Gruppieren Sie die Startkonfigurationen mit gleichem Startverhalten.

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

Detaillierte Informationen zum Thema

- Synchronisation in die Exchange Online-Umgebung konfigurieren auf Seite 30
- Schema aktualisieren auf Seite 30

Synchronisation in die Exchange Online-Umgebung konfigurieren

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

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

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Prüfen Sie, ob die bestehenden Mappings für die Synchronisation in das Zielsystem genutzt werden können. Erstellen Sie bei Bedarf neue Mappings.
3. Erstellen Sie mit dem Workflowassistenten einen neuen Workflow.

   Es wird ein Workflow mit der Synchronisationsrichtung **In das Zielsystem** angelegt.
4. Erstellen Sie eine neue Startkonfiguration. Nutzen Sie dabei den neu angelegten Workflow.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

Schema aktualisieren

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

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

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

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

Um das Schema einer Systemverbindung zu aktualisieren

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

   - ODER -

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

   Die Schemadaten werden neu geladen.

Um ein Mapping zu bearbeiten

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

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

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

Nachbehandlung ausstehender Objekte

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

Ausstehende Objekte

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

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

Führen Sie dafür einen Zielsystemabgleich durch.

Um ausstehende Objekte nachzubearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Zielsystemabgleich: Exchange Online**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp **Exchange Online** als Synchronisationstabellen zugewiesen sind.
2. Öffnen Sie auf dem Formular **Zielsystemabgleich**, in der Spalte **Tabelle/Objekt** den Knoten der Tabelle, für die sie ausstehende Objekte nachbearbeiten möchten.

   Es werden alle Objekte angezeigt, die als ausstehend markiert sind. Die Spalten **Letzter Protokolleintrag** und **Letzte ausgeführte Methode** zeigen den Zeitpunkt für den letzten Eintrag im Synchronisationsprotokoll und die dabei ausgeführte Verarbeitungsmethode. Der Eintrag **Kein Protokoll verfügbar** hat folgende Bedeutungen:
   - Das Synchronisationsprotokoll wurde bereits gelöscht.

     - ODER -
   - Im Zielsystem wurde eine Zuweisung aus einer Mitgliederliste gelöscht.

     Bei der Synchronisation wird das Basisobjekt der Zuordnung aktualisiert. Dafür erscheint ein Eintrag im Synchronisationsprotokoll. Der Eintrag in der Zuordnungstabelle wird als ausstehend markiert, es gibt jedoch keinen Eintrag im Synchronisationsprotokoll.
   - Im Zielsystem wurde ein Objekt gelöscht, das eine Mitgliederliste enthält.

     Bei der Synchronisation werden das Objekt und alle zugehörigen Einträge in Zuordnungstabellen als ausstehend markiert. Ein Eintrag im Synchronisationsprotokoll erscheint jedoch nur für das gelöschte Objekt.

   TIPP:

   Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

   a. Wählen Sie auf dem Formular für den Zielsystemabgleich das Objekt.

   b. Öffnen Sie das Kontextmenü und klicken Sie **Objekt anzeigen**.
3. Wählen Sie die Objekte, die Sie nachbearbeiten möchten. Mehrfachauswahl ist möglich.
4. Klicken Sie in der Formularsymbolleiste eins der folgenden Symbole, um die

jeweilige Methode auszuführen.

Tabelle 7: Methoden zur Behandlung ausstehender Objekte

Symbol	Methode	Beschreibung
	Löschen	Das Objekt wird sofort in der One Identity Manager-Datenbank gelöscht. Eine Löschverzögerung wird nicht berücksichtigt. Die Markierung **Ausstehend** wird für das Objekt entfernt. Indirekte Mitgliedschaften können nicht gelöscht werden.
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung **Ausstehend** wird für das Objekt entfernt. Die Methode löst das Ereignis `HandleOutstanding` aus. Dadurch wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt. Voraussetzungen: • Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen. • Der Zielsystemkonnektor kann schreibend auf das Zielsystem zugreifen.
	Zurücksetzen	Die Markierung **Ausstehend** wird für das Objekt entfernt.

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

HINWEIS: Standardmäßig werden die ausgewählten Objekte parallel verarbeitet. Damit wird die Ausführung der ausgewählten Methode beschleunigt. Wenn bei der Verarbeitung ein Fehler auftritt, wird die Aktion abgebrochen und alle Änderungen werden rückgängig gemacht.

Um den Fehler zu lokalisieren, muss die Massenverarbeitung der Objekte deaktiviert werden. Die Objekte werden damit nacheinander verarbeitet. Das fehlerhafte Objekt wird in der Fehlermeldung benannt. Alle Änderungen, die bis zum Auftreten des Fehlers vorgenommen wurden, werden gespeichert.

Um die Massenverarbeitung zu deaktivieren

- Deaktivieren Sie in der Formularsymbolleiste  .

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

Um kundenspezifische Tabellen in den Zielsystemabgleich aufzunehmen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Exchange 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. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Exchange Online**.
3. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
4. Wählen Sie die Zuordnungstabellen, für die Sie die Einzelprovisionierung

ermöglichen möchten. Mehrfachauswahl ist möglich.

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

5. Klicken Sie **Merge-Modus**.
6. Speichern Sie die Änderungen.

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

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

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

Um die Standardbedingung wiederherzustellen

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

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

Beschleunigung der Provisionierung und Einzelobjektsynchronisation

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

HINWEIS: Die Lastverteilung sollte nicht permanent für Provisionierungen oder Einzelobjektsynchronisationen eingesetzt werden. Durch die parallele Verarbeitung der Objekte kann es beispielsweise vorkommen, dass Abhängigkeiten nicht aufgelöst

werden, da die referenzierten Objekte von einem anderen Jobserver noch nicht vollständig verarbeitet wurden.

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

Um die Lastverteilung zu konfigurieren

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

   Alle Jobserver müssen auf den gleichen Azure Active Directory Mandanten zugreifen können, wie der Synchronisationsserver für das jeweilige Basisobjekt.
2. Weisen Sie im Synchronization Editor an das Basisobjekt eine kundendefinierte Serverfunktion zu.

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

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

   Ausführliche Informationen zur Bearbeitung von Basisobjekten finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.
3. Weisen Sie diese Serverfunktion im Manager an alle Jobserver zu, welche die Prozesse zur Provisionierung und Einzelobjektsynchronisation für das Basisobjekt verarbeiten sollen.

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

   Ausführliche Informationen zur Bearbeitung von Servern finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung*.

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

Um den Synchronisationsserver ohne Lastverteilung zu nutzen

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

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

Unterstützung bei der Analyse von Synchronisationsproblemen

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

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

Um den Synchronisationsanalysebericht zu erstellen

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

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

Deaktivieren der Synchronisation

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

Um regelmäßige Synchronisationen zu verhindern

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

   Synchronisationen können nun nur noch manuell gestartet werden.

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

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

Um das Synchronisationsprojekt zu deaktivieren

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

Verwandte Themen

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Exchange Online-Umgebung auf Seite 17

3

Basisdaten für die Verwaltung einer Exchange Online-Umgebung

Für die Verwaltung einer Exchange 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 Konfigurationsparameter für die Verwaltung einer Exchange Online-Umgebung auf Seite 62.

- Kontendefinitionen

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

  Weitere Informationen finden Sie unter Einrichten von Kontendefinitionen auf Seite 40.

- 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 31.

- Zielsystemverantwortliche

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

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

  Weitere Informationen finden Sie unter Zielsystemverantwortliche auf Seite 59.

Einrichten von Kontendefinitionen

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

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

Ausführliche Informationen zu Kontendefinitionen finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

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

Erstellen einer Kontendefinition

Um eine Kontendefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | 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.

HINWEIS: Exchange Online Benutzerpostfächer werden über die Zuweisung und das Entfernen von Lizenzen über Azure Active Directory Abonnements im Azure Active Directory Modul erstellt beziehungsweise gelöscht werden. Weitere Informationen finden Sie im One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung.

Detaillierte Informationen zum Thema

- Stammdaten einer Kontendefinition auf Seite 41

Verwandte Themen

Verarbeitung von Systemobjekten

Stammdaten einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 8: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte Kontendefinition	Vorausgesetzte Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch mitbestellt oder zugeordnet.

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

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

Erstellen der Automatisierungsgrade

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

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

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

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

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

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

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

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

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Automatisierungsgrade zuweisen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Automatisierungsgrade zu.

   - ODER -

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

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

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | 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 45

Stammdaten eines Automatisierungsgrades

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 9: Stammdaten eines Automatisierungsgrades

Eigenschaft	Beschreibung
Automatisierungsgrad	Bezeichnung des Automatisierungsgrades.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Betriebsdaten überschreibend	Angabe, ob Daten an Benutzerkonten, die sich aus den IT Betriebsdaten bilden, automatisch aktualisiert werden. Zulässige Werte sind: • **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.

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

Erstellen einer Abbildungsvorschrift für IT Betriebsdaten

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

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

- Gruppen erbbar

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **IT Betriebsdaten Abbildungsvorschrift bearbeiten** und erfassen Sie folgende Informationen.

Tabelle 10: Abbildungsvorschrift für IT Betriebsdaten

Eigenschaft	Beschreibung
Spalte	Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.
Quelle	Angabe, welche Rolle verwendet wird, um die Eigenschaften für das Benutzerkonto zu ermitteln. Zur Auswahl stehen: • Primäre Abteilung • Primärer Standort • Primäre Kostenstelle • Primäre Geschäftsrolle HINWEIS: Verwenden Sie die primäre Geschäftsrolle nur, wenn das Geschäftsrollenmodul vorhanden ist. • keine Angabe Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option **Immer Standardwert verwenden** setzen.
Standardwert	Standardwert der Eigenschaft für das Benutzerkonto einer Person, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann.
Immer Standardwert verwenden	Angabe, ob die Eigenschaft des Benutzerkontos immer mit dem Standardwert besetzt wird. Es erfolgt keine dynamische Ermittlung der IT Betriebsdaten aus einer Rolle.
Benachrichtigung bei Verwendung des Standards	Angabe, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkontos mit Standardwerten** verwendet. Um die Mailvorlage zu ändern, passen Sie den Konfigurationsparameter **TargetSystem | AzureAD | ExchangeOnline | Accounts | MailTemplateDefaultValues** an.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Erfassen der IT Betriebsdaten auf Seite 48

Erfassen der IT Betriebsdaten

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

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

Beispiel

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

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

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

Um IT Betriebsdaten festzulegen

1. Wählen Sie im Manager in der Kategorie **Organisationen** oder **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten**.

3. Klicken Sie **Hinzufügen** und erfassen Sie die folgenden Daten.

Tabelle 11: IT Betriebsdaten

Eigenschaft	Beschreibung
Wirksam für	Anwendungsbereich der IT Betriebsdaten. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden. Um den Anwendungsbereich festzulegen a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. b. Wählen Sie unter **Tabelle** die Tabelle, die das Zielsystem abbildet oder für eine Kontendefinition die Tabelle `TSBAccountDef`. c. Wählen Sie unter **Wirksam für** das konkrete Zielsystem oder die konkrete Kontendefinition. d. Klicken Sie **OK**.
Spalte	Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.
Wert	Konkreter Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Erstellen einer Abbildungsvorschrift für IT Betriebsdaten auf Seite 46

IT Betriebsdaten ändern

Sobald sich die IT Betriebsdaten ändern, müssen Sie diese Änderungen für bestehende Benutzerkonten übernehmen. Dafür führen Sie die Bildungsregeln an den betroffenen Spalten erneut aus. Bevor Sie die Bildungsregeln ausführen, prüfen Sie, welche Auswirkungen eine Änderung der IT Betriebsdaten auf bestehende Benutzerkonten hat. Für jede betroffene Spalte an jedem betroffenen Benutzerkonto können Sie entscheiden, ob die Änderung in die One Identity Manager-Datenbank übernommen werden soll.

Voraussetzungen

- Die IT Betriebsdaten einer Abteilung, einer Kostenstelle, einer Geschäftsrolle oder eines Standorts wurden geändert.

  - ODER -

- Die Standardwerte in der IT Betriebsdaten Abbildungsvorschrift für eine Kontendefinition wurden geändert.

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

Um die Bildungsregeln auszuführen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Bildungsregeln ausführen**.

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

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

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

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinition an Personen

Kontendefinitionen werden an die Personen des Unternehmens zugewiesen.

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

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

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

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

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

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

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

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

Detaillierte Informationen zum Thema

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 51
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 52
- Kontendefinition an alle Personen zuweisen auf Seite 53
- Kontendefinition direkt an Personen zuweisen auf Seite 53
- Zuweisen der Kontendefinition an ein Zielsystem auf Seite 56

Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.

3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
    - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
    - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
    - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

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

    Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinition an Geschäftsrollen zuweisen auf Seite 52
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 52
- Kontendefinition direkt an Personen zuweisen auf Seite 53

Kontendefinition an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

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

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

    Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 51
- Kontendefinition an alle Personen zuweisen auf Seite 53
- Kontendefinition direkt an Personen zuweisen auf Seite 53

Kontendefinition an alle Personen zuweisen

Um eine Kontendefinition an alle Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | 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 51
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 52
- Kontendefinition direkt an Personen zuweisen auf Seite 53

Kontendefinition direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

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

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Person und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 51
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 52
- Kontendefinition an alle Personen zuweisen auf Seite 53

Kontendefinition an Systemrollen zuweisen

Installierte Module: Systemrollenmodul

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

Um Kontendefinitionen in eine Systemrolle aufzunehmen

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

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Kontendefinition in den IT Shop aufnehmen

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

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

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien

zusammengestellt. Damit die Kontendefinition im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.

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

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

Um eine Kontendefinition in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen** (bei rollenbasierter Anmeldung).

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

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

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

Verwandte Themen

- Stammdaten einer Kontendefinition auf Seite 41
- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 51
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 52
- Kontendefinition direkt an Personen zuweisen auf Seite 53
- Kontendefinition an Systemrollen zuweisen auf Seite 54

Zuweisen der Kontendefinition an ein Zielsystem

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

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

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

Um die Kontendefinition an ein Zielsystem zuzuweisen

1. Wählen Sie im Manager in der Kategorie **Azure Active Directory | Mandanten** den Mandanten.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie in der Auswahlliste **Kontendefinition (initial)** die Kontendefinition für die Benutzerkonten.

4. Wählen Sie in der Auswahlliste **E-Mail Kontaktdefinition (initial)** die Kontendefinition für die E-Mail Kontakte.
5. Wählen Sie in der Auswahlliste **E-Mail Benutzerdefinition (initial)** die Kontendefinition für die E-Mail Benutzer.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Zuweisen der Kontendefinition an Personen auf Seite 50

Löschen einer Kontendefinition

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

Um eine Kontendefinition zu löschen

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Personen.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Deaktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.
    e. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Personen.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **An Personen zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Personen.
    e. Speichern Sie die Änderungen.
3. Entfernen Sie die Zuordnung der Kontendefinition zu Abteilungen, Kostenstellen und Standorten.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Organisationen zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Abteilungen,

Kostenstellen und Standorte.

e. Speichern Sie die Änderungen.

4. Entfernen Sie die Zuordnung der Kontendefinition zu Geschäftsrollen.
   a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
   b. Wählen Sie in der Ergebnisliste die Kontendefinition.
   c. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.

      Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
   d. Speichern Sie die Änderungen.
5. Wenn die Kontendefinition über den IT Shop bestellt wurde, muss sie abbestellt und aus allen IT Shop Regalen entfernt werden.

   Ausführliche Informationen zum Abbestellen einer Bestellung finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

   Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen
   a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

      - ODER -

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

      Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.
6. Entfernen Sie die Zuordnung der Kontendefinition als vorausgesetzte Kontendefinition einer anderen Kontendefinition. Solange die Kontendefinition Voraussetzung einer anderen Kontendefinition ist, kann sie nicht gelöscht werden. Prüfen Sie alle Kontendefinitionen.
   a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
   b. Wählen Sie in der Ergebnisliste die Kontendefinition.
   c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
   d. Entfernen Sie in der Auswahlliste **Vorausgesetzte Kontendefinition** die Kontendefinition.
   e. Speichern Sie die Änderungen.

7. Entfernen Sie die Zuordnung der Kontendefinition zum Zielsystem.
    a. Wählen Sie im Manager in der Kategorie **Azure Active Directory | Mandanten** den Mandanten.
    b. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    c. Entfernen Sie auf dem Tabreiter **Allgemein** die zugewiesenen Kontendefinitionen.
    d. Speichern Sie die Änderungen.
8. Löschen Sie die Kontendefinition.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Klicken Sie , um die Kontendefinition zu löschen.

Zielsystemverantwortliche

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

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

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

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

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

    Zielsystemverantwortliche der Standardanwendungsrolle sind berechtigt alle Exchange Online Objekte 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 12: Standardanwendungsrolle für Zielsystemverantwortliche

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

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 | Exchange 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 **Azure Active Directory | Basisdaten zur Konfiguration | Zielsystemverantwortliche** die Anwendungsrolle.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Personen zu und speichern Sie die Änderungen.

Um Zielsystemverantwortliche für einzelne Mandanten festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **Azure Active Directory | 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 (Exchange Online)** die Anwendungsrolle.

   - ODER -

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

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

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

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer Exchange Online-Umgebung auf Seite 6

Anhang A

Konfigurationsparameter für die Verwaltung einer Exchange Online-Umgebung

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

Tabelle 13: Konfigurationsparameter für die Verwaltung einer Exchange Online-Umgebung

Konfigurationsparameter	Bedeutung
TargetSystem | AzureAD | ExchangeOnline	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung des Zielsystems Exchange Online. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.
TargetSystem | AzureAD | ExchangeOnline | Accounts	Der Konfigurationsparameter erlaubt die Konfiguration der Angaben zu Empfängern.
TargetSystem | AzureAD | ExchangeOnline | Accounts | MailTemplateDefaultValues	Der Konfigurationsparameter enthält die Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto mit Standardwerten** verwendet.
TargetSystem | AzureAD | ExchangeOnline | Defaul-tAddress	Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem | AzureAD | ExchangeOnline | 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

Konfigurationsparameter	Bedeutung
	werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.

Anhang B

Standardprojektvorlagen für Exchange 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 14: Abbildung der Exchange Online Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im Exchange Online	Tabelle im One Identity Manager Schema
DistributionGroup	O3EDL
DynamicDistributionGroup	O3EDynDL
Mailbox	O3EMailbox
MailContact	O3EMailContact
MailPublicFolder	O3EMailPublicFolder
MailUser	O3EMailUser
MobileDeviceMailboxPolicy	O3EMobileDeviceMBPolicy
OWAMailboxPolicy	O3EOwaMailboxPolicy
PublicFolder	O3EPublicFolder
RententionPolicy	O3ERetentionPolicy
RoleAssignmentPolicy	O3ERoleAssignmentPolicy
SharingPolicy	O3ESharingPolicy
UnifiedGroup	O3EUnifiedGroup

Anhang C

Verarbeitung von Systemobjekten

Folgende Tabelle beschreibt die zulässigen Verarbeitungsmethoden für die Schematypen von Exchange Online und benennt notwendige Einschränkungen bei der Verarbeitung der Systemobjekte.

Das Hinzufügen und Löschen von Benutzerpostfächer kann in One Identity Manager nur über Abonnementzuweisungen in Azure Active Directory verarbeitet werden. Dadurch entsteht ein Postfach, das erst nach Synchronisation in der Datenbank erscheint. Danach kann es automatisch in Exchange Online provisioniert werden.

Tabelle 15: Zulässige Verarbeitungsmethoden für Schematypen

Typ	Lesen	Hinzufügen	Löschen	Aktualisieren
Richtlinie für Rollen-zuweisungen	Ja	Nein	Nein	Nein
Postfachrichtlinie für mobile Geräte	Ja	Nein	Nein	Nein
Freigaberichtlinie	Ja	Nein	Nein	Nein
Aufbewahrungsrichtlinie	Ja	Nein	Nein	Nein
Outlook Web App-Postfachrichtlinie	Ja	Nein	Nein	Nein
Öffentlicher Ordner	Ja	Nein	Nein	Nein
E-Mail-aktivierter öffent-licher Ordner	Ja	Nein	Nein	Nein
Ressourcenpostfach	Ja	Ja	Ja	Ja
Freigegebenes Postfach	Ja	Ja	Ja	Ja
Benutzerpostfach	Ja	Nein	Nein	Nein
E-Mail-Kontakt	Ja	Ja	Ja	Ja
E-Mail-Benutzer	Ja	Ja	Ja	Ja
Verteilergruppe	Ja	Ja	Ja	Ja

Typ	Lesen	Hinzufügen	Löschen	Aktualisieren
Dynamische Verteiler-gruppe	Ja	Nein	Ja	Ja
Office 365-Gruppe	Ja	Ja	Ja	Ja

Über uns

One Identity Lösungen eliminieren die Komplexität und die zeitaufwendigen Prozesse, die häufig bei der Identity Governance, der Verwaltung privilegierter Konten und dem Zugriffsmanagement aufkommen. Unsere Lösungen fördern die Geschäftsagilität und bieten durch lokale, hybride und Cloud-Umgebungen eine Möglichkeit zur Bewältigung Ihrer Herausforderungen beim Identitäts- und Zugriffsmanagement.

Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen, wie Lizenzierungen, Support oder Support-Erneuerungen, besuchen Sie https://www.oneidentity.com/company/contact-us.aspx.

Technische Supportressourcen

Technische Unterstützung steht für One Identity Kunden mit einem gültigen Wartungsvertrag und Kunden mit Testversionen zur Verfügung. Sie können auf das Support Portal unter https://support.oneidentity.com/ zugreifen.

Das Support Portal bietet Selbsthilfe-Tools, die Sie verwenden können, um Probleme schnell und unabhängig zu lösen, 24 Stunden am Tag, 365 Tage im Jahr. Das Support Portal ermöglicht Ihnen:

- Senden und Verwalten von Serviceanfragen
- Anzeigen von Knowledge Base Artikeln
- Anmeldung für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Videos unter www.YouTube.com/OneIdentity
- Engagement in der One Identity Community
- Chat mit Support-Ingenieuren
- Anzeigen von Diensten, die Sie bei Ihrem Produkt unterstützen

Index

L

M

O

P

S

Z