One Identity Manager 9.2

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 - 29. September 2023, 04:47 Uhr

Die aktuellsten Versionen der Produktdokumentation finden Sie unter One Identity Manager Dokumentation.

Inhalt

Über dieses Handbuch

Das *One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung* beschreibt, wie Sie die Synchronisation einer Exchange Online-Umgebung mit dem One Identity Manager einrichten. Sie erfahren, wie Sie mit dem One Identity Manager die Postfächer, E-Mail Benutzer, E-Mail Kontakte, E-Mail-aktivierte Verteilergruppen und Office 365 Gruppen Exchange Online-Umgebung verwalten.

Dieses Handbuch wurde als Nachschlagewerk für End-Anwender, Systemadministratoren, Berater, Analysten und andere IT-Fachleute entwickelt.

HINWEIS: Dieses Handbuch beschreibt die Funktionen des One Identity Manager, die für den Standardbenutzer verfügbar sind. Abhängig von der Systemkonfiguration und den Berechtigungen stehen Ihnen eventuell nicht alle Funktionen zur Verfügung.

Verfügbare Dokumentation

Die One Identity Manager Dokumentation erreichen Sie im Manager und im Designer über das Menü **Hilfe** > **Suchen**. Die Online Version der One Identity Manager Dokumentation finden Sie im Support-Portal unter Online-Dokumentation. Videos mit zusätzlichen Informationen finden Sie unter www.YouTube.com/OneIdentity.

2

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*.

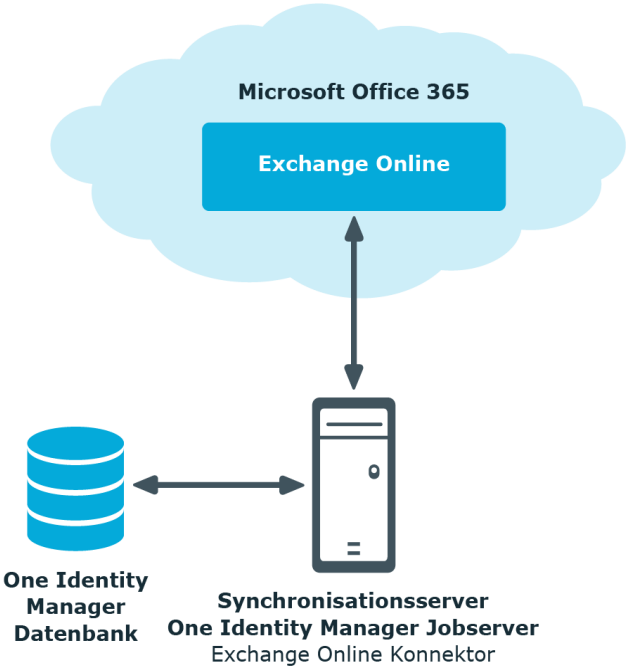
HINWEIS: Voraussetzung für die Verwaltung einer Exchange Online-Umgebung im One Identity Manager ist die Installation des Exchange Online Moduls. Ausführliche Informationen zur Installation finden Sie im *One Identity Manager Installationshandbuch.*

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. Für den Zugriff auf die Exchange Online Daten wird das Exchange Online PowerShell V3 Modul verwendet.

Für den Zugriff auf die Daten einer Exchange Online Organisation muss das Zielsystem Azure Active Directory, in dem sich die Exchange Online Organisation 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 Identitäten 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. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Identitäten anlegen, die nicht den Identitätstyp **Primäre Identität** haben. • 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 Identitäten als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung an den

Benutzer	Aufgaben
	Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.

Konfigurationsparameter für die Verwaltung von Exchange Online-Umgebungen

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 207.

Synchronisieren einer Exchange Online-Umgebung

HINWEIS: Die Synchronisation folgender Cloudbereitstellungen mit dem Exchange Online Konnektor wird unterstützt.

- Microsoft 365 Global Service
- Microsoft 365 GCC High

Für den Abgleich der Informationen zwischen der One Identity Manager-Datenbank und einer Exchange Online-Umgebung sorgt der One Identity Manager Service.

Informieren Sie sich hier:

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

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

Detaillierte Informationen zum Thema

- Einrichten der Synchronisation mit einer Exchange Online-Umgebung auf Seite 15
- Anpassen einer Synchronisationskonfiguration auf Seite 36
- Ausführen einer Synchronisation auf Seite 49
- Aufgaben nach einer Synchronisation auf Seite 54
- Fehleranalyse auf Seite 57
- Datenfehler bei der Synchronisation ignorieren auf Seite 58
- Verarbeitung von Exchange Online Systemobjekten auf Seite 211

Einrichten der Synchronisation mit einer Exchange Online-Umgebung

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

Voraussetzungen für die Synchronisation einer Exchange Online-Umgebung sind:

- Der Azure Active Directory Mandant ist im One Identity Manager bekannt.
- Die Synchronisation der Azure Active Directory-Umgebung wird regelmäßig ausgeführt.

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

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.

      HINWEIS: Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
    - Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.
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 16
- Einrichten des Exchange Online Synchronisationsservers auf Seite 19
- Vorbereiten der administrativen Arbeitsstation für den Zugriff auf die Exchange Online-Umgebung auf Seite 24
- Vorbereiten eines Remoteverbindungsservers für den Zugriff auf die Exchange Online-Umgebung auf Seite 25
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Exchange Online-Umgebung auf Seite 26
- Besonderheiten zur Synchronisation von Exchange Online-Umgebungen auf Seite 33
- Anpassen einer Synchronisationskonfiguration auf Seite 36
- Konfigurationsparameter für die Verwaltung einer Exchange Online-Umgebung auf Seite 207
- Standardprojektvorlagen für Exchange Online auf Seite 210

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

Zugriff auf Exchange Online über Benutzerkonto
oder
Nur-App-Authentifizierung
	Für die Synchronisation mit einer Exchange Online Umgebung wird die Authentifizierung über ein Benutzerkonto mit ausreichenden Berechtigungen oder die Nur-App-Authentifizierung über ein selbstsigniertes Zertifikat unterstützt.
	• Für die Authentifizierung mit einem definierten Benutzerkonto stellen Sie ein Benutzerkonto bereit, das mindestens die folgenden Berechtigungen besitzt.
	  • Mitglied der Exchange Online Rollengruppe **Recipient Management**
	  • Mitglied der Exchange Online Rollengruppe **Records Management**

Benutzer	Berechtigungen
	• Mitglied der Exchange Online Rollengruppe **View-Only Organization Management** • Mitglied der Exchange Online Rolle **Security Group Creation and Membership** HINWEIS: Erstellen Sie im Exchange Online eine neue Rollengruppe. Weisen Sie dieser Rollengruppe die Rolle und das Benutzerkonto zu. • Mitglied in der Azure Active Directory Administratorrolle **Gruppenadministrator** HINWEIS: Das Benutzerkonto für den Zugriff auf Exchange Online darf keine Multifaktor-Authentifizierung nutzen, damit automatisierte Anmeldungen in einem Benutzerkontext möglich sind. Für die Zuweisungen der Exchange Online Rollengruppen an das Benutzerkonto nutzen Sie das Exchange Admin Center. Die Zuweisung der Azure Active Directory Administratorrolle an das Benutzerkonto nehmen Sie im Azure Active Directory Admin Center vor. Die Admin Center erreichen Sie beispielsweise über https://admin.microsoft.com/. Ausführliche Informationen zum Verwalten von Berechtigungen in Exchange Online und in Azure Active Directory finden Sie in der *Microsoft Dokumentation*. • Für die Nur-App-Authentifizierung über ein selbstsigniertes Zertifikat registrieren und konfigurieren Sie eine Anwendung für Exchange Online PowerShell im Azure Active Directory Mandanten. HINWEIS: Das Anlegen und Bearbeiten von **O3EUnifiedGroups** ist über eine Nur-App-Authentifizierung nicht möglich. Um diese Berechtigungen nutzen zu können ist eine Authentifizierung mit einem Benutzerkonto notwendig. Wie Sie die Nur-App-Authentifizierung einrichten, finden Sie unter Einrichten einer Nur-App-Authentifizierung.

Benutzer	Berechtigungen
	• Für den Exchange Online Konnektor weisen Sie an die Anwendung mindestens die Azure Active Directory Administratorrollen **Globaler Administrator** und **Exchange-Administrator** zu.
Benutzerkonto des One Identity Manager Service	Das Benutzerkonto für den One Identity Manager Service benötigt die Benutzerrechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Verzeichnisse und Dateien anlegen und bearbeiten. Das Benutzerkonto muss der Gruppe **Domänen-Benutzer** angehören. Das Benutzerkonto benötigt das erweiterte Benutzerrecht **Anmelden als Dienst**. Das Benutzerkonto benötigt Berechtigungen für den internen Webservice. HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so können Sie die Berechtigungen für den internen Webservice über folgenden Kommandozeilenaufruf vergeben: `netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"` Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis. In der Standardinstallation wird der One Identity Manager installiert unter: • `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen) • `%ProgramFiles%\One Identity` (auf 64-Bit Betriebssystemen)
Benutzer für den Zugriff auf die One Identity Manager-Datenbank	Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer **Synchronization** bereitgestellt.

Exchange Online PowerShell V3 Modul installieren

Der Exchange Online Konnektor verwendet das Exchange Online PowerShell V3 Modul für den Zugriff auf die Daten einer Exchange Online-Umgebung.

- Das Exchange Online PowerShell V3 Modul muss auf dem Synchronisationsserver installiert werden.
- Erfolgt der direkte Zugriff auf die Exchange Online-Umgebung von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, muss auf dieser Arbeitsstation das Exchange Online PowerShell V3 Modul installiert werden.
- Ist der direkte Zugriff auf die Exchange Online-Umgebung von der Arbeitsstation nicht möglich, können Sie einen Remoteverbindungsserver einrichten. Auf dem Remoteverbindungsserver muss das Exchange Online PowerShell V3 Modul installiert werden.

Ausführliche Informationen zu den Voraussetzungen und zur Installation des Exchange Online PowerShell V3 Moduls finden Sie in der Exchange Online PowerShell Dokumentation von Microsoft.

Verwandte Themen

- Einrichten des Exchange Online Synchronisationsservers auf Seite 19
- Vorbereiten der administrativen Arbeitsstation für den Zugriff auf die Exchange Online-Umgebung auf Seite 24
- Vorbereiten eines Remoteverbindungsservers für den Zugriff auf die Exchange Online-Umgebung auf Seite 25

Einrichten des Exchange Online Synchronisationsservers

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

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

WICHTIG:

- Der Exchange Online Konnektor verwendet das Exchange Online PowerShell V3 Modul für den Zugriff auf die Daten einer Exchange Online-Umgebung. Das Exchange Online PowerShell V3 Modul muss auf dem Synchronisationsserver

installiert werden.

- Wenn Sie für die Authentifizierung des Exchange Online Konnektors am Exchange Online die Nur-App-Authentifizierung über ein selbstsigniertes Zertifikat verwenden möchten, dann muss das Zertifikat auf dem Synchronisationsserver in den Zertifikatsspeicher des Benutzers installiert werden, unter dem der One Identity Manager Service läuft.

Detaillierte Informationen zum Thema

- Systemanforderungen für den Exchange Online Synchronisationsserver auf Seite 20
- Exchange Online PowerShell V3 Modul installieren auf Seite 19
- One Identity Manager Service mit Exchange Online Konnektor installieren auf Seite 21
- Benutzer und Berechtigungen für die Synchronisation mit einer Exchange Online-Umgebung auf Seite 16

Systemanforderungen für den Exchange Online Synchronisationsserver

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 Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
- Microsoft .NET Framework Version 4.8 oder höher

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.
- Windows PowerShell 5.1 oder höher
- Exchange Online PowerShell Modul Version 3.2.0 oder höher

Verwandte Themen

- Exchange Online PowerShell V3 Modul installieren auf Seite 19
- One Identity Manager Service mit Exchange Online Konnektor installieren auf Seite 21

One Identity Manager Service mit Exchange Online Konnektor installieren

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

Tabelle 3: Eigenschaften des Jobservers

Eigenschaft	Wert
Serverfunktion	Exchange Online Konnektor
Maschinenrolle	Server | Job Server | Exchange Online

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

Um einen Jobserver einzurichten, führen Sie folgende Schritte aus.

1. Erstellen Sie einen Jobserver und installieren und konfigurieren Sie den One Identity Manager Service.

   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.
   - Installation der One Identity Manager Service-Komponenten entsprechend der Maschinenrollen.
   - Konfigurieren des One Identity Manager Service.
   - Starten des One Identity Manager Service.

   Mit dem Server Installer können Sie den One Identity Manager Service lokal oder remote installieren.

   Für die Remote-Installation des One Identity Manager Service stellen Sie eine administrative Arbeitstation bereit, auf der die One Identity Manager-Komponenten installiert sind. Für eine lokale Installation stellen Sie sicher, dass die One Identity Manager-Komponenten auf dem Server installiert sind. Ausführliche Informationen zur Installation der One Identity Manager-Komponenten finden Sie im *One Identity Manager Installationshandbuch*.

2. Wenn Sie mit einer verschlüsselten One Identity Manager-Datenbank arbeiten, geben Sie dem One Identity Manager Service den Datenbankschlüssel bekannt. Ausführliche Informationen zum Arbeiten mit einer verschlüsselten

One Identity Manager-Datenbank finden Sie im *One Identity Manager Installationshandbuch*.

3. 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 Erfassen der Verbindungsinformationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

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

1. Starten Sie das Programm Server Installer.

   HINWEIS: Für eine Remote-Installation starten Sie das Programm Server Installer auf Ihrer administrativen Arbeitsstation. Für eine lokale Installation starten Sie das Programm auf dem Server.

2. Auf der Seite **Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.

   Für die Verbindung zur Datenbank können Sie eine Verbindung über den Anwendungsserver oder die direkte Verbindung verwenden.

3. Auf der Seite **Servereigenschaften** legen Sie fest, auf welchem Server der One Identity Manager Service installiert werden soll.

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

      - ODER -

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

   b. Bearbeiten Sie folgende Informationen für den Jobserver.

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

        Syntax:

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

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

4. Auf der Seite **Maschinenrollen** wählen Sie **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 in der Modulliste **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.
   d. Klicken Sie **OK**.

   Für eine Verbindung zum Anwendungsserver:

   a. Wählen Sie in der Modulliste den Eintrag **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen**.
   b. Wählen Sie **AppServerJobProvider** und klicken Sie **OK**.
   c. Wählen Sie in der Modulliste **Prozessabholung > AppServerJobProvider**.
   d. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
   e. Erfassen Sie die Adresse (URL) zum Anwendungsserver und klicken Sie **OK**.
   f. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
   g. Wählen Sie unter **Authentifizierungsverfahren** das Authentifizierungsmodul für die Anmeldung. 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*.
   h. Klicken Sie **OK**.
7. Zur Konfiguration der Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.
10. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.

- **Computer**: Wählen Sie den Server über die Auswahlliste oder erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.

  Um die Installation lokal auszuführen, wählen Sie in der Auswahlliste den Eintrag **<lokale Installation>**.
- **Dienstkonto**: Erfassen Sie die Angaben zum Benutzerkonto unter dem der One Identity Manager Service läuft. Erfassen Sie das Benutzerkonto, das Kennwort zum Benutzerkonto und die Kennwortwiederholung.

Die Installation des Dienstes erfolgt mit dem Benutzerkonto, mit dem Sie an der administrativen Arbeitsstation angemeldet sind. Möchten Sie ein anderes Benutzerkonto für die Installation des Dienstes nutzen, können Sie dieses in den erweiterten Optionen eintragen.

Angaben zum One Identity Manager Service können Sie ebenfalls über die erweiterten Optionen ändern, beispielsweise das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den One Identity Manager Service.

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

    Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.
12. Auf der letzten Seite des Server Installer klicken Sie **Fertig**.

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

Vorbereiten der administrativen Arbeitsstation für den Zugriff auf die Exchange Online-Umgebung

Um im Synchronization Editor die Synchronisation mit einer Exchange Online-Umgebung zu konfigurieren, muss der One Identity Manager Daten direkt aus der Exchange Online-Umgebung auslesen. Erfolgt der direkte Zugriff auf die Exchange Online-Umgebung von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, muss auf dieser Arbeitsstation zusätzlich die folgende Software installiert sein:

- Windows PowerShell Version 5.1 oder höher
- Exchange Online PowerShell Modul Version 3.2.0 oder höher

Ist der direkte Zugriff auf die Exchange Online-Umgebung von der Arbeitsstation nicht möglich, können Sie einen Remoteverbindungsserver einrichten.

Verwandte Themen

- Exchange Online PowerShell V3 Modul installieren auf Seite 19
- Benutzer und Berechtigungen für die Synchronisation mit einer Exchange Online-Umgebung auf Seite 16
- Vorbereiten eines Remoteverbindungsservers für den Zugriff auf die Exchange Online-Umgebung auf Seite 25

Vorbereiten eines Remoteverbindungsservers für den Zugriff auf die Exchange Online-Umgebung

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

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

Konfiguration des Remoteverbindungsservers:

- One Identity Manager Service ist gestartet
- **RemoteConnectPlugin** ist installiert
- Windows PowerShell 5.1 oder höher ist installiert
- Exchange Online PowerShell V2 Modul 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 das **RemoteConnectPlugin** zusätzlich installieren.

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

Verwandte Themen

- Einrichten des Exchange Online Synchronisationsservers auf Seite 19
- Exchange Online PowerShell V3 Modul installieren auf Seite 19

- One Identity Manager Service mit Exchange Online Konnektor installieren auf Seite 21
- Benutzer und Berechtigungen für die Synchronisation mit einer Exchange Online-Umgebung auf Seite 16
- Vorbereiten der administrativen Arbeitsstation für den Zugriff auf die Exchange Online-Umgebung auf Seite 24

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. Ausführliche Informationen zur Einrichtung der Synchronisation finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

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

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.

HINWEIS: Beachten Sie bei der Einrichtung der Synchronisation die unter Besonderheiten zur Synchronisation von Exchange Online-Umgebungen auf Seite 33 beschriebenen Empfehlungen.

Voraussetzungen für die Erstellung eines Synchronisationsprojektes

- Der Azure Active Directory Mandant ist im One Identity Manager bekannt.
- Die Synchronisation der Azure Active Directory-Umgebung wird regelmäßig ausgeführt.

Verwandte Themen

- Benötigte Informationen für Synchronisationsprojekte mit Exchange Online auf Seite 27
- Initiales Synchronisationsprojekt für eine Exchange Online-Umgebung erstellen auf Seite 28
- Besonderheiten zur Synchronisation von Exchange Online-Umgebungen auf Seite 33

- Anpassen einer Synchronisationskonfiguration auf Seite 36
- Standardprojektvorlagen für Exchange Online auf Seite 210
- Einstellungen des Exchange Online Konnektors auf Seite 213

Benötigte Informationen für Synchronisationsprojekte mit Exchange Online

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

Tabelle 4: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen

Informationen zur Authentifizierung	Für die Synchronisation mit einer Exchange Online Umgebung wird die Authentifizierung über ein Benutzerkonto mit ausreichenden Berechtigungen oder die Nur-App-Authentifizierung über ein selbstsigniertes Zertifikat unterstützt.
	Weitere Informationen finden Sie unter Benutzer und Berechtigungen für die Synchronisation mit einer Exchange Online-Umgebung auf Seite 16.
	Benötigte Informationen für die Authentifizierung mit einem Benutzerkonto:
	• Benutzerkonto und Kennwort zur Authentifizierung am Exchange Online.
	Beispiel:
	`<user>@<domain.com>`
	`sync.user@<yourorganization>.onmicrosoft.com`
	Benötigte Informationen für die Authentifizierung über ein selbstsigniertes Zertifikat (Nur-App-Authentifizierung):
	• Anwendungs-ID, die beim Registrieren der Anwendung für Exchange Online PowerShell im Azure Active Directory Mandanten erzeugt wird.
	• Fingerabdruck des selbstsignierten Zertifikates
	Wie Sie die Nur-App-Authentifizierung einrichten, finden Sie unter Einrichten einer Nur-App-Authentifizierung.

Organisationsdomäne	Azure Active Directory Name der Domäne zur Anmeldung am Azure Active Directory.

Angaben	Erläuterungen
	Beispiel: `<yourorganization>.onmicrosoft.com`
Synchronisationsserver für Exchange Online	Vom Synchronisationsserver werden alle Aktionen des One Identity Manager Service gegen die Zielsystemumgebung ausgeführt. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet. Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem Exchange Online Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften. • Serverfunktion: **Exchange Online Konnektor** • Maschinenrolle: **Server | Job Server | Exchange Online** Weitere Informationen finden Sie unter Einrichten des Exchange Online Synchronisationsservers auf Seite 19.
Verbindungsdaten zur One Identity Manager-Datenbank	• Datenbankserver • Name der Datenbank • SQL Server-Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung verwendet wird Die Verwendung der integrierten Windows-Authentifizierung wird nicht empfohlen. Sollten Sie das Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
Remoteverbindungsserver	Weitere Informationen finden Sie unter Vorbereiten eines Remoteverbindungsservers für den Zugriff auf die Exchange Online-Umgebung auf Seite 25.

Initiales Synchronisationsprojekt für eine Exchange Online-Umgebung erstellen

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

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

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

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

   Der Projektassistent des Synchronization Editors wird gestartet.

3. Auf der Startseite des Projektassistenten klicken Sie **Weiter**.
4. 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.

5. Auf der Seite **Bereitstellung/Organisationsdomäne** erfassen Sie folgende Informationen.
   - **Bereitstellung**: Wählen Sie die Cloudbereitstellung, in der Ihre Exchange Online-Umgebung betrieben wird. Zur Auswahl stehen **Microsoft 365 global service** und **Microsoft 365 GCC High**.
   - **Organisationsdomäne**: Geben Sie den Azure Active Directory Namen der Domäne an.

     Beispiel:

     `<yourorganization>.onmicrosoft.com`

6. Auf der Seite **Verbindungsparameter** erfassen Sie die Anmeldeinformationen für die Verbindung zum Exchange Online.
   - Wenn die Authentifizierung mit einem definierten Benutzerkonto erfolgen soll, erfassen Sie folgende Informationen.

- **Benutzername**: Erfassen Sie den vollqualifizierten Name (FQDN) des Benutzerkonto zur Anmeldung.

  Beispiel:

  `<user>@<domain.com>`

  `sync.user@<yourorganization>.onmicrosoft.com`
- **Kennwort**: Erfassen Sie das Kennwort zum Benutzerkonto.

- Wenn die Authentifizierung über ein selbstsigniertes Zertifikat erfolgen soll (die Nur-App-Authentifizierung), erfassen Sie folgende Informationen.
  - **Anwendungs-ID**: Anwendungs-ID, die beim Registrieren der Anwendung für Exchange Online PowerShell im Azure Active Directory Mandanten erzeugt wird.
  - **Zertifikat Fingerabdruck**: Fingerabdruck des selbstsignierten Zertifikates.

Klicken Sie ☑ um die Verbindungsparameter zu testen.

HINWEIS:

- Über die Schaltfläche **Satz hinzufügen** können Sie weitere Verbindungsparameter eingeben. Diese Verbindungsparameter werden vom Exchange Online Konnektor zyklisch abgefragt, wenn Anfragen an Exchange Online gesendet werden. Durch die Verwendung mehrerer Verbindungssätze wird der Einschränkungsgrenzwert langsamer erreicht.

  Ausführliche Information zur Einschränkungsgrenzwerte in Exchange Online finden Sie in der *Dokumentation von Microsoft*.
- Wenn Sie die Authentifizierung über ein selbstsigniertes Zertifikat einsetzen, dann müssen Sie sicherstellen, dass pro Verbindungssatz eine eigene Anwendungsregistrierung vorhanden ist. Das gleiche Zertifikat darf nicht mehrfach für verschiedene Anwendungsregistrierungen verwendet werden.
- Klicken Sie ☑ **Alle Sätze prüfen** um die Verbindungsparameter alle Sätze auf einmal zu prüfen.

7. Auf der letzten Seite des Systemverbindungsassistenten klicken Sie **Fertig** um zum Projektassistenten zurückzukehren.
8. Auf der Seite **One Identity Manager Verbindung** überprüfen Sie die Verbindungsdaten zur One Identity Manager-Datenbank. Die Daten werden aus der verbundenen Datenbank geladen. Geben Sie das Kennwort erneut ein.

   HINWEIS:

   - Wenn Sie mit einer unverschlüsselten One Identity Manager-Datenbank arbeiten und noch kein Synchronisationsprojekt in der Datenbank gespeichert ist, erfassen Sie alle Verbindungsdaten neu.
   - Wenn bereits ein Synchronisationsprojekt gespeichert ist, wird diese Seite nicht angezeigt.
9. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des

Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.

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

Tabelle 5: Zielsystemzugriff festlegen

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

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

    Wenn der Synchronisationsserver noch nicht als Jobserver für dieses Zielsystem 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.

> TIPP: Sie können auch einen vorhandenen Jobserver zusätzlich als Synchronisationsserver für dieses Zielsystem einsetzen.
>
> - Um einen Jobserver auszuwählen, klicken Sie .
>
> Diesem Jobserver wird die passende Serverfunktion automatisch zugewiesen.

c. Klicken Sie **OK**.

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

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

12. 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**.
> - 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.
> - Die Verbindungsdaten zum Zielsystem werden in einem Variablenset gespeichert und können bei Bedarf im Synchronization Editor in der Kategorie **Konfiguration > Variablen** angepasst werden.

Verwandte Themen

- Benutzer und Berechtigungen für die Synchronisation mit einer Exchange Online-Umgebung auf Seite 16
- Benötigte Informationen für Synchronisationsprojekte mit Exchange Online auf Seite 27
- Einrichten des Exchange Online Synchronisationsservers auf Seite 19
- Synchronisationsprotokoll konfigurieren auf Seite 35
- Anpassen einer Synchronisationskonfiguration auf Seite 36

- Ausführen einer Synchronisation auf Seite 49
- Aufgaben nach einer Synchronisation auf Seite 54
- Standardprojektvorlagen für Exchange Online auf Seite 210
- Einstellungen des Exchange Online Konnektors auf Seite 213

Besonderheiten zur Synchronisation von Exchange Online-Umgebungen

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

Abhängigkeitsauflösung

Die automatische Abhängigkeitsauflösung für Synchronisationsschritte 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 Standardprojektvorlage für Exchange Online unterstützt die Konvertierung von 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 manuell gelöst werden.

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

Statistikdaten über Postfachnutzung synchronisieren

Die Statistikdaten über die Postfachnutzung werden in einem eigenen Synchronisationsschritt 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 einem Postfach.
DeletedItemCount	Anzahl der gelöschten Elemente.
DumpsterMessagesPerFolderCountReceiveQuota	Maximale Anzahl an Nachrichten, die ein Ordner im Ordner **Wiederherstellbare Elemente** enthalten darf.
DumpsterMessagesPerFolderCountWarningQuota	Anzahl der Elemente, die ein Ordner im Ordner **Wiederherstellbare Elemente** enthalten darf, bevor der Benutzer eine Warnung erhält.
ItemCount	Anzahl der Nachrichten in einem 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 40.

Synchronisationsprotokoll konfigurieren

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

Um den Inhalt des Synchronisationsprotokolls für eine Systemverbindung zu konfigurieren

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

   - ODER -

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

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

Um den Inhalt des Synchronisationsprotokolls für einen Synchronisationsworkflow zu konfigurieren

1. Wählen Sie im Synchronization Editor die Kategorie **Workflows**.
2. Wählen Sie in der Navigationsansicht einen Workflow.
3. Wählen Sie den Bereich **Allgemein** und klicken Sie **Bearbeiten**.
4. Wählen Sie den Tabreiter **Synchronisationsprotokoll**.
5. Aktivieren Sie die zu protokollierenden Daten.

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

6. Klicken Sie **OK**.

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

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

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 52

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 bei der Synchronisation den One Identity Manager als primäres System zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um allgemeingültige Synchronisationskonfigurationen zu erstellen, die erst beim Start der Synchronisation die notwendigen Informationen über die zu synchronisierenden Objekte erhalten, können Variablen eingesetzt werden. Variablen können beispielsweise in den Basisobjekten, den Schemaklassen oder den Verarbeitungsmethoden eingesetzt werden.
- 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.

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

Detaillierte Informationen zum Thema

- Besonderheiten zur Synchronisation von Exchange Online-Umgebungen auf Seite 33
- Synchronisation in die Exchange Online-Umgebung konfigurieren auf Seite 37
- Einstellungen der Systemverbindung zur Exchange Online-Umgebung ändern auf Seite 38
- Schema aktualisieren auf Seite 43
- Beschleunigung der Exchange Online Synchronisation durch Revisionsfilterung auf Seite 44
- Provisionierung von Mitgliedschaften konfigurieren auf Seite 45
- Einzelobjektsynchronisation konfigurieren auf Seite 47
- Beschleunigung der Provisionierung und Einzelobjektsynchronisation auf Seite 48

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

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

Einstellungen der Systemverbindung zur Exchange Online-Umgebung ändern

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

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

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

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

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

Detaillierte Informationen zum Thema

- Verbindungsparameter im Variablenset bearbeiten auf Seite 38
- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 39
- Erweiterte Einstellungen für den Exchange Online Konnektor auf Seite 40
- Einstellungen des Exchange Online Konnektors auf Seite 213

Verbindungsparameter im Variablenset bearbeiten

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

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

Um die Verbindungsparameter in einem spezialisierten Variablenset anzupassen

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

Einige Verbindungsparameter können hier in Variablen umgewandelt werden. Für andere sind bereits Variablen angelegt.

4. Wählen Sie einen Parameter und klicken Sie **Umwandeln**.
5. Wählen Sie die Kategorie **Konfiguration > Variablen**.

   Im unteren Bereich der Dokumentenansicht werden alle spezialisierten Variablensets angezeigt.
6. Wählen Sie ein spezialisiertes Variablenset oder klicken Sie in der Symbolleiste der Variablensetansicht .
   - Um das Variablenset umzubenennen, markieren Sie das Variablenset und klicken Sie in der Symbolleiste der Variablensetansicht . Erfassen Sie einen Namen für das Variablenset.
7. Wählen Sie die zuvor angelegten Variablen und erfassen Sie neue Werte.
8. Wählen Sie die Kategorie **Konfiguration > Startkonfigurationen**.
9. Wählen Sie eine Startkonfiguration und klicken Sie **Bearbeiten**.
10. Wählen Sie den Tabreiter **Allgemein**.
11. Ordnen Sie im Eingabefeld **Variablenset** das spezialisierte Variablenset zu.
12. Wählen Sie die Kategorie **Konfiguration > Basisobjekte**.
13. Wählen Sie ein Basisobjekt und klicken Sie .

    - ODER -

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

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

Verwandte Themen

- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 39

Eigenschaften der Zielsystemverbindung bearbeiten

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

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

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

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

Um die Verbindungsparameter mit dem Systemverbindungsassistenten zu bearbeiten

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

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

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

Verwandte Themen

- Verbindungsparameter im Variablenset bearbeiten auf Seite 38

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 **3** Verbindungen pro Benutzer zu.

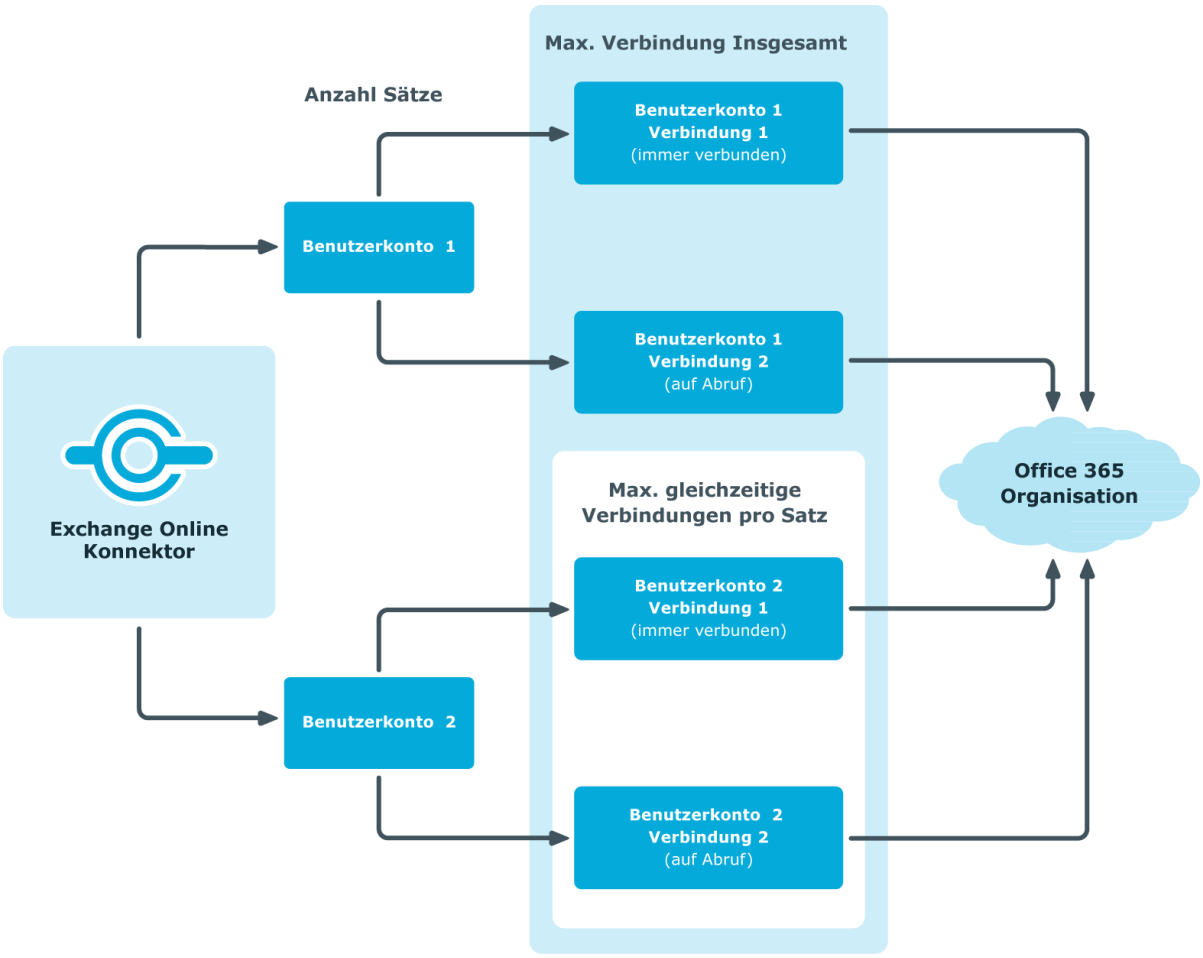
Wenn sich der Exchange Online Konnektor verbindet, erstellt er eine Windows PowerShell Sitzung pro Verbindungsparametersatz unabhängig von der Anzahl der anschließenden Anfragen. Weitere Verbindungen werden dynamisch hinzugefügt falls sie benötigt werden, zum Beispiel beim Laden mehrerer Objekte während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

Abbildung 2: Ermittlung der Sitzungen



Um die Anzahl der gleichzeitigen Verbindungen zu ändern

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

   Der Systemverbindungsassistent wird gestartet.
3. Auf der Startseite des Systemverbindungsassistenten aktivieren Sie **Erweiterte Einstellungen anzeigen**.
4. Auf der Seite Erweiterte Einstellungen geben Sie im **Eingabefeld gleichzeitige Verbindungen pro Verbindungsparametersatz** einen Wert zwischen **1** und **3** ein.
5. Folgen Sie den weiteren Anweisungen des Systemverbindungsassistenten.
6. Speichern Sie die Änderungen.

Anpassen der Konnektordefinition

VORSICHT: 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.

WICHTIG: Anpassungen an der Konnektordefinition sollten nur temporär genutzt werden, um bei Bedarf Problem zu umgehen.

WICHTIG: Eine angepasste Konnektordefinition wird nicht standardmäßig überschrieben, wenn eine neue Version des Konnektors beziehungsweise eine aktualisierte Konnektordefinition herausgegeben wird. Es werden keine Patches angewendet.

Wenn Sie die Konnektordefinition anpassen, müssen Sie bei Bedarf Ihre Änderungen manuell auf eine neue Version des Konnektors beziehungsweise eine aktualisierte Konnektordefinition übernehmen.

Mit dieser Einstellung kann die Definition angepasst werden, die vom Konnektor verwendet wird, um beispielsweise Ein- und Ausgaben zwischen den Exchange Online Cmdlets und dem Schema der Synchronization Engine umzusetzen.

Um die Konnektordefinition anzupassen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
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. Folgen Sie den weiteren Anweisungen des Systemverbindungsassistenten.
7. Speichern Sie die Änderungen.

Schema aktualisieren

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

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

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

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

Um das Schema einer Systemverbindung zu aktualisieren

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

- ODER -

Wählen Sie die Kategorie **Konfiguration > One Identity Manager Verbindung**.

3. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Die Schemadaten werden neu geladen.

Um ein Mapping zu bearbeiten

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

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

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

Beschleunigung der Exchange Online Synchronisation durch Revisionsfilterung

Beim Start der Synchronisation werden alle zu synchronisierenden Objekte geladen. Ein Teil dieser Objekte wurde gegebenenfalls seit der letzten Synchronisation nicht geändert und muss daher bei der Synchronisation nicht verarbeitet werden. Indem nur solche Objekte geladen werden, die sich seit der letzten Synchronisation geändert haben, kann die Synchronisation beschleunigt werden. Zur Beschleunigung der Synchronisation nutzt der One Identity Manager die Revisionsfilterung.

Exchange Online unterstützt die Revisionsfilterung für die Schematypen `Mailbox`, `MailUser`, `MailContact`, `MailPublicFolder`, `DistributionGroup`, `DynamicDistributionGroup` und `UnifiedGroup`.

Wie die Änderungszeitpunkte für die Revisionsfilterung ermittelt werden, konfigurieren Sie über die folgenden Verbindungsparameter im Synchronisationsprojekt.

- **Verwende lokale Serverzeit als Revision**: Ist der Wert **True**, wird die lokale Serverzeit des Synchronisationsservers für die Revisionsfilterung genutzt (Standard). Damit ist es nicht erforderlich Zielsystemobjekte zur Revisionsbestimmung zu laden. Ist der Wert **False**, wird das Änderungsdatum der zugrunde liegenden Azure Active Directory Objekte für die Revisionsfilterung verwendet.

  Variable: `CP_UseLocalServerTimeAsRevision`
- **Max. Zeitabweichung (lokal/remote) in Minuten**: Angabe der maximalen Zeitdifferenz in Minuten zwischen dem Synchronisationsserver und dem

Exchange Online Server. Standardwert sind 60 Minuten. Ist die Zeitdifferenz größer als 60 Minuten, passen Sie den Wert an.

Variable: `CP_LocalServerRevisionMaxDifferenceInMinutes`

Der Zeitpunkt, der sich aus der lokalen Serverzeit und der maximalen Zeitabweichung ergibt, wird als Revision in der One Identity Manager-Datenbank (Tabelle `DPRRevisionStore`, Spalte `Value`) gespeichert. Wird nicht die lokale Serverzeit verwendet, erfolgt die Ermittlung der Revision aus den Änderungszeitpunkten der Objekte.

Dieser Wert wird als Vergleichswert für die Revisionsfilterung bei der nächsten Synchronisation mit dem selben Workflow genutzt. Beim nächsten Synchronisationslauf werden nur noch jene Objekte gelesen, die sich seit diesem Datum verändert haben. Anhand des Vergleichs werden unnötige Aktualisierungen von Objekten, die sich seit dem letzten Synchronisationslauf nicht verändert haben, vermieden.

Die Revision wird zu Beginn einer Synchronisation ermittelt. Objekte, die durch die Synchronisation geändert werden, werden bei der nächsten Synchronisation nochmals geladen und überprüft. Die zweite Synchronisation nach der Initialsynchronisation ist daher noch nicht deutlich schneller.

Die Revisionsfilterung kann an den Workflows oder an den Startkonfigurationen zugelassen werden.

Um die Revisionsfilterung an einem Workflow zuzulassen

- Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
- Bearbeiten Sie die Eigenschaften des Workflows. Wählen Sie in der Auswahlliste **Revisionsfilterung** den Eintrag **Revisionsfilter nutzen**.

Um die Revisionsfilterung an einer Startkonfiguration zuzulassen

- Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
- Bearbeiten Sie die Eigenschaften der Startkonfiguration. Wählen Sie in der Auswahlliste **Revisionsfilterung** den Eintrag **Revisionsfilter nutzen**.

Ausführliche Informationen zur Revisionsfilterung sowie zur Anpassung der Verbindungsparameter und zur Bearbeitung von Variablen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Einstellungen der Systemverbindung zur Exchange Online-Umgebung ändern auf Seite 38

Provisionierung von Mitgliedschaften konfigurieren

Mitgliedschaften, beispielsweise von Benutzerkonten in Gruppen, werden in der One Identity Manager-Datenbank in Zuordnungstabellen gespeichert. Bei der

Provisionierung von geänderten Mitgliedschaften werden möglicherweise Änderungen, die im Zielsystem vorgenommen wurden, überschrieben. Dieses Verhalten kann unter folgenden Bedingungen auftreten:

- Mitgliedschaften werden im Zielsystem in Form einer Liste als Eigenschaft eines Objekts gespeichert.

  Beispiel: Liste von Postfächern in der Eigenschaft `AcceptMessagesOnlyFrom` eines Exchange Online Postfachs (`Mailbox`)
- 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.
5. Klicken Sie **Merge-Modus**.

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

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

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

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

Um die originale Bedingung wiederherzustellen

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

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

Beispiel für eine Bedingung an der Zuordnungstabelle `O3EUnifiedGroupAcceptRcpt`:

```
exists (select top 1 1 from O3EUnifiedGroup g
     where g.UID_O3EUnifiedGroup = i.UID_O3EUnifiedGroup
     and <einschränkende Bedingung>)
```

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

Einzelobjektsynchronisation konfigurieren

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

Voraussetzungen

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

Für Synchronisationsprojekte, die mit der Standard-Projektvorlage erstellt wurden, ist die Einzelobjektsynchronisation vollständig konfiguriert. Wenn Sie kundenspezifische Tabellen in solch ein Synchronisationsprojekt einbeziehen möchten, müssen Sie die Einzelobjektsynchronisation für diese Tabellen konfigurieren. Ausführliche Informationen

dazu finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

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

1. Wählen Sie im Manager die Kategorie **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 kundenspezifische Tabelle zu, für die Sie die Einzelobjektsynchronisation nutzen möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die kundenspezifische Tabelle und erfassen Sie den **Pfad zum Basisobjekt**.

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

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

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 53
- Ausstehende Objekte nachbehandeln auf Seite 54

Beschleunigung der Provisionierung und Einzelobjektsynchronisation

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

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

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

Um die Lastverteilung zu konfigurieren

1. Konfigurieren Sie die Server und geben Sie diese im One Identity Manager als Jobserver bekannt.
    - Für Jobserver, die an der Lastverteilung teilnehmen, muss die Option **Keine Prozesszuteilung** deaktiviert sein.
    - Weisen Sie diesen Jobservern die Serverfunktion **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.

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

Um den Synchronisationsserver ohne Lastverteilung zu nutzen

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

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

Detaillierte Informationen zum Thema

- Jobserver für Exchange Online-spezifische Prozessverarbeitung auf Seite 88

Ausführen einer Synchronisation

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

Synchronisation irregulär abgebrochen wurde, müssen Sie die Startinformation zurücksetzen, um die Synchronisation erneut starten zu können.

Wenn verschiedene Zielsysteme immer in einer vorher festgelegten Reihenfolge synchronisiert werden sollen, nutzen Sie Startfolgen, um die Synchronisation zu starten. In einer Startfolge können beliebige Startkonfigurationen aus verschiedenen Synchronisationsprojekten zusammengestellt und in eine Ausführungsreihenfolge gebracht werden. Ausführliche Informationen zu Startfolgen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Detaillierte Informationen zum Thema

- Synchronisationen starten auf Seite 50
- Synchronisation deaktivieren auf Seite 51
- Synchronisationsergebnisse anzeigen auf Seite 52
- Einzelobjekte synchronisieren auf Seite 53
- Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) auf Seite 59

Synchronisationen starten

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

Um regelmäßige Synchronisationen auszuführen

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

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

Um die initiale Synchronisation manuell zu starten

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

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

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

Synchronisation deaktivieren

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

Um regelmäßige Synchronisationen zu verhindern

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

   Synchronisationen können nun nur noch manuell gestartet werden.

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

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

Um das Synchronisationsprojekt zu deaktivieren

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

Verwandte Themen

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Exchange Online-Umgebung auf Seite 26
- Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) auf Seite 59

Synchronisationsergebnisse anzeigen

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

Um das Protokoll einer Synchronisation anzuzeigen

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

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

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

Um das Protokoll einer Provisionierung anzuzeigen

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

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

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

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

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

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.

Einzelobjekte synchronisieren

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

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

Um ein Einzelobjekt zu synchronisieren

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

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

Besonderheiten bei der Synchronisation von Mitgliederlisten

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

Beispiel:

Basisobjekt für die Zuweisung von Empfangsbeschränkungen für Exchange Online E-Mail Benutzer und E-Mail-aktivierte Verteilergruppen ist die Verteilergruppe.

Im Zielsystem wurde für eine E-Mail-aktivierte Verteilergruppe die Postannahme für einen E-Mail Benutzer erlaubt. Um diese Zuweisung zu synchronisieren, wählen Sie im Manager diese Verteilergruppe und führen Sie die Einzelobjektsynchronisation aus. Dabei werden alle Zuweisungen für diese Verteilergruppe synchronisiert.

Der E-Mail Benutzer muss in der One Identity Manager-Datenbank bereits als Objekt vorhanden sein, damit die Zuweisung angelegt werden kann.

Detaillierte Informationen zum Thema

- Einzelobjektsynchronisation konfigurieren auf Seite 47

Aufgaben nach einer Synchronisation

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

- Ausstehende Objekte nachbehandeln auf Seite 54
- Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen auf Seite 56
- Exchange Online E-Mail Benutzer und Exchange Online E-Mail Kontakte über Kontendefinitionen verwalten auf Seite 57

Ausstehende Objekte nachbehandeln

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

Ausstehende Objekte

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

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

Führen Sie dafür einen Zielsystemabgleich durch.

Um ausstehende Objekte nachzubearbeiten

1. Wählen Sie im Manager die Kategorie **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

1. Wählen Sie auf dem Formular für den Zielsystemabgleich das Objekt.
2. Öffnen Sie das Kontextmenü und klicken Sie **Objekt anzeigen**.

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

Tabelle 6: Methoden zur Behandlung ausstehender Objekte

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

TIPP: Wenn eine Methode wegen bestimmter Einschränkungen nicht ausgeführt werden kann, ist das jeweilige Symbol deaktiviert.

- Um Details zur Einschränkung anzuzeigen, klicken Sie in der Spalte **Einschränkungen** die Schaltfläche **Anzeigen**.

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

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

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

Um die Massenverarbeitung zu deaktivieren

- Deaktivieren Sie in der Formularsymbolleiste das Symbol .

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

Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen

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

Um kundenspezifische Tabellen in den Zielsystemabgleich aufzunehmen

1. Wählen Sie im Manager die Kategorie **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.

Verwandte Themen

- Ausstehende Objekte nachbehandeln auf Seite 54

Exchange Online E-Mail Benutzer und Exchange Online E-Mail Kontakte über Kontendefinitionen verwalten

Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Exchange Online E-Mail Benutzer und Exchange Online E-Mail Kontakte Identitäten erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für die Exchange Online Organisation bekannt, werden die E-Mail Benutzer und E-Mail Kontakte mit den Identitäten verbunden. Es wird jedoch noch keine Kontendefinition zugewiesen. Die E-Mail Benutzer und E-Mail Kontakte sind somit im Zustand **Linked** (verbunden).

Um die E-Mail Benutzer und E-Mail Kontakte über Kontendefinitionen zu verwalten, weisen Sie eine Kontendefinition und einen Automatisierungsgrad zu.

Um die Exchange Online E-Mail Benutzer und E-Mail Kontakte über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie dem Azure Active Directory Mandanten die Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand **Linked** (verbunden) die Kontendefinition und den Automatisierungsgrad zu.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Benutzer > Verbunden aber nicht konfiguriert > <Azure Active Directory Mandant>**.

       - ODER -

       Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Kontakte > Verbunden aber nicht konfiguriert > <Azure Active Directory Mandant>**.
    b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.

Verwandte Themen

- Kontendefinitionen für Exchange Online E-Mail Benutzer und Exchange Online E-Mail Kontakte auf Seite 64
- Kontendefinitionen an Azure Active Directory Mandanten zuweisen auf Seite 82

Fehleranalyse

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

- Synchronisation simulieren

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

- Synchronisation analysieren

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

- Meldungen protokollieren

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

- Startinformation zurücksetzen

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

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

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 52

Datenfehler bei der Synchronisation ignorieren

Standardmäßig werden Objekte mit fehlerhaften Daten nicht synchronisiert. Diese Objekte können synchronisiert werden, sobald die fehlerhaften Daten korrigiert wurden. In einzelnen Situationen kann es notwendig sein, solche Objekte dennoch zu synchronisieren und nur die fehlerhaften Objekteigenschaften zu ignorieren. Dieses Verhalten kann für die Synchronisation in den One Identity Manager konfiguriert werden.

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

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

   Der Systemverbindungsassistent wird gestartet.

4. Auf der Seite **Weitere Einstellungen** aktivieren Sie **Versuche Datenfehler zu ignorieren**.

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

   Fehler in Standardspalten, wie Primärschlüssel oder UID-Spalten, und Pflichteingabespalten können nicht ignoriert werden.

5. Speichern Sie die Änderungen.

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

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

Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus)

Wenn ein Zielsystemkonnektor das Zielsystem zeitweilig nicht erreichen kann, können Sie den Offline-Modus für dieses Zielsystem aktivieren. Damit können Sie verhindern, dass zielsystemspezifische Prozesse in der Jobqueue eingefroren werden und später manuell reaktiviert werden müssen.

Ob der Offline-Modus für eine Zielsystemverbindung grundsätzlich verfügbar ist, wird am Basisobjekt des jeweiligen Synchronisationsprojekts festgelegt. Sobald ein Zielsystem tatsächlich nicht erreichbar ist, kann diese Zielsystemverbindungen über das Launchpad offline und anschließend wieder online geschaltet werden.

Im Offline-Modus werden alle dem Basisobjekt zugewiesenen Jobserver angehalten. Dazu gehören der Synchronisationsserver und alle an der Lastverteilung beteiligten Jobserver. Falls einer der Jobserver auch andere Aufgaben übernimmt, dann werden diese ebenfalls nicht verarbeitet.

Voraussetzungen

Der Offline-Modus kann nur unter bestimmten Voraussetzungen für ein Basisobjekt zugelassen werden.

- Der Synchronisationsserver wird für kein anderes Basisobjekt als Synchronisationsserver genutzt.
- Wenn dem Basisobjekt eine Serverfunktion zugewiesen ist, darf keiner der Jobserver mit dieser Serverfunktion eine andere Serverfunktion (beispielsweise Aktualisierungsserver) haben.

- Es muss ein dedizierter Synchronisationsserver eingerichtet sein, der ausschließlich die Jobqueue für dieses Basisobjekt verarbeitet. Gleiches gilt für alle Jobserver, die über die Serverfunktion ermittelt werden.

Um den Offline-Modus für ein Basisobjekt zuzulassen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Basisobjekte**.
3. Wählen Sie in der Dokumentenansicht das Basisobjekt und klicken Sie .
4. Aktivieren Sie **Offline-Modus verfügbar**.
5. Klicken Sie **OK**.
6. Speichern Sie die Änderungen.

WICHTIG: Um Dateninkonsistenzen zu vermeiden, sollten Offline-Phasen kurz gehalten werden.

Die Zahl der nachträglich zu verarbeitenden Prozesse ist abhängig vom Umfang der Änderungen in der One Identity Manager-Datenbank mit Auswirkungen auf das Zielsystem während der Offline-Phase. Um Datenkonsistenz zwischen One Identity Manager-Datenbank und Zielsystem herzustellen, müssen alle anstehenden Prozesse verarbeitet werden, bevor eine Synchronisation gestartet wird.

Nutzen Sie den Offline-Modus möglichst nur, um kurzzeitige Systemausfälle, beispielsweise Wartungsfenster, zu überbrücken.

Um ein Zielsystem als offline zu kennzeichnen

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie **Verwalten > Systemüberwachung > Zielsysteme als offline kennzeichnen**.
3. Klicken Sie **Starten**.

   Der Dialog **Offline-Systeme verwalten** wird geöffnet. Im Bereich **Basisobjekte** werden die Basisobjekte aller Zielsystemverbindungen angezeigt, für die der Offline-Modus zugelassen ist.
4. Wählen Sie das Basisobjekt, dessen Zielsystemverbindung nicht verfügbar ist.
5. Klicken Sie **Offline schalten**.
6. Bestätigen Sie die Sicherheitsabfrage mit **OK**.

   Damit werden die dem Basisobjekt zugewiesenen Jobserver angehalten. Es werden keine Synchronisations- und Provisionierungsaufträge ausgeführt. In Job Queue Info wird angezeigt, wenn ein Jobserver offline geschaltet wurde und die entsprechenden Aufträge nicht verarbeitet werden.

Ausführliche Informationen zum Offline-Modus finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Synchronisation deaktivieren auf Seite 51

Basisdaten für die Verwaltung einer Exchange Online-Umgebung

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

- Kontendefinitionen

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

  Weitere Informationen finden Sie unter Kontendefinitionen für Exchange Online E-Mail Benutzer und Exchange Online E-Mail Kontakte auf Seite 64.

- Kennwortrichtlinien

  Der One Identity Manager unterstützt Sie beim Erstellen von komplexen Kennwortrichtlinien beispielsweise für Systembenutzerkennwörter, das zentrale Kennwort von Identitäten sowie für Kennwörter für die einzelnen Zielsysteme. Kennwortrichtlinien werden sowohl bei der Eingabe eines Kennwortes durch den Anwender als auch bei der Generierung von Zufallskennwörtern angewendet.

  In der Standardinstallation werden vordefinierte Kennwortrichtlinien mitgeliefert, die Sie nutzen können und bei Bedarf an Ihre Anforderungen anpassen können. Zusätzlich können Sie eigene Kennwortrichtlinien definieren.

  Für die Verwendung von Kennwortrichtlinien werden die Konfigurationseinstellungen für Azure Active Directory genutzt. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung.*

- Initiales Kennwort für neue E-Mail Benutzer

  Um das initiale Kennwort für E-Mail Benutzer zu vergeben, stehen Ihnen verschiedene Möglichkeiten zur Verfügung. Tragen Sie beim Erstellen eines E-Mail Benutzers ein Kennwort ein oder verwenden Sie ein zufällig generiertes initiales Kennwort.

  Für die Generierung von Zufallskennwörtern für neue E-Mail Benutzer werden die Konfigurationseinstellungen für Azure Active Directory genutzt. Ausführliche

Informationen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung.*

- E-Mail-Benachrichtigungen über die Anmeldeinformationen

  Bei Erstellung eines neuen E-Mail Benutzers werden die Anmeldeinformationen an definierte Empfänger versendet. Dabei werden zwei Benachrichtigungen versendet, die den Benutzernamen und das initiale Kennwort enthalten. Zur Erzeugung der Benachrichtigungen werden Mailvorlagen genutzt.

  Für das Versenden der Anmeldeinformationen werden die Konfigurationseinstellungen für Azure Active Directory genutzt. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung.*

- Zielsystemtypen

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

  Weitere Informationen finden Sie unter Ausstehende Objekte nachbehandeln auf Seite 54.

- Zielsystemverantwortliche

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

  Wenn Sie die Berechtigungen 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 für Exchange Online auf Seite 85.

- Server

  Für die Verarbeitung der Exchange Online-spezifischen Prozesse im One Identity Manager müssen die Server mit ihren Serverfunktionen bekannt sein. Dazu gehört beispielsweise der Synchronisationsserver.

  Weitere Informationen finden Sie unter Jobserver für Exchange Online-spezifische Prozessverarbeitung auf Seite 88.

Kontendefinitionen für Exchange Online E-Mail Benutzer und Exchange Online E-Mail Kontakte

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

Um E-Mail Benutzer oder E-Mail Kontakte automatisch an Identitäten zu vergeben, kennt der One Identity Manager Kontendefinitionen. Kontendefinitionen können für jedes Zielsystem erzeugt werden. Hat eine Identität noch keinen E-Mail Benutzer oder E-Mail Kontakt in einem Zielsystem, wird durch die Zuweisung der Kontendefinition an eine Identität ein neuer E-Mail Benutzer oder ein neuer E-Mail Kontakt erzeugt.

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 von Kontendefinitionen
- Konfigurieren der Automatisierungsgrade
- Erstellen der Abbildungsvorschriften für die IT Betriebsdaten
- Erfassen der IT Betriebsdaten
- Zuweisen der Kontendefinitionen an Identitäten und Zielsysteme

Detaillierte Informationen zum Thema

- Kontendefinitionen erstellen auf Seite 65
- Kontendefinitionen bearbeiten auf Seite 65
- Stammdaten für Kontendefinitionen auf Seite 66
- Automatisierungsgrade bearbeiten auf Seite 68
- Automatisierungsgrade erstellen auf Seite 69
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 69
- Stammdaten für Automatisierungsgrade auf Seite 70
- Abbildungsvorschrift für IT Betriebsdaten erstellen auf Seite 71
- IT Betriebsdaten erfassen auf Seite 72
- IT Betriebsdaten ändern auf Seite 74
- Zuweisen der Kontendefinitionen an Identitäten auf Seite 75
- Kontendefinitionen an Azure Active Directory Mandanten zuweisen auf Seite 82
- Kontendefinitionen löschen auf Seite 83

Kontendefinitionen erstellen

Erstellen Sie eine oder mehrere Kontendefinitionen für das Zielsystem.

Um eine Kontendefinition zu erstellen

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

Detaillierte Informationen zum Thema

- Stammdaten für Kontendefinitionen auf Seite 66
- Kontendefinitionen bearbeiten auf Seite 65
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 69

Kontendefinitionen bearbeiten

Sie können die Stammdaten der Kontendefinitionen bearbeiten.

Um eine Kontendefinition zu bearbeiten

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. Bearbeiten Sie die Stammdaten der Kontendefinition.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Kontendefinitionen auf Seite 66
- Kontendefinitionen erstellen auf Seite 65
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 69

Stammdaten für Kontendefinitionen

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 7: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die E-Mail Benutzer oder die E-Mail Kontakte abbildet. Für Exchange Online E-Mail Benutzer wählen Sie **O3EMailUser**. Für Exchange Online E-Mail Kontakte wählen Sie **O3EMailContact**.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte Kontendefinition	Angabe der vorausgesetzten Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch zugeordnet. Für Exchange Online lassen Sie die Angabe leer.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatisierungsgrad (initial)	Standardautomatisierungsgrad, der bei Neuanlage von E-Mail Benutzern oder E-Mail Kontakten standardmäßig verwendet werden soll.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Kontendefinition an Identitäten. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Leistungsposition	Leistungsposition, über welche die Kontendefinition im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.
IT Shop	Gibt an, ob die Kontendefinition über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Identitäten und Rollen außerhalb des IT Shop zugewiesen werden.

Eigenschaft	Beschreibung
Verwendung nur im IT Shop	Gibt an, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal 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 Identitäten	Gibt an, ob die Kontendefinition automatisch an alle internen Identitäten zugewiesen werden soll. Um die Kontendefinition automatisch an alle internen Identitäten zuzuweisen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Identitäten aktivieren**. Die Kontendefinition wird an jede Identität zugewiesen, die nicht als extern markiert ist. Sobald eine neue interne Identität erstellt wird, erhält diese Identität ebenfalls automatisch diese Kontendefinition. Um die automatische Zuweisung der Kontendefinition von allen Identitäten zu entfernen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Identitäten deaktivieren**. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Identitäten zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.
Kontendefinition bei dauerhafter Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Identitäten. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Der E-Mail Benutzer oder der E-Mail Kontakt bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Der zugehörige E-Mail Benutzer oder der zugehörige E-Mail Kontakt wird deaktiviert.
Kontendefinition bei zeitweiliger Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Identitäten. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Der E-Mail Benutzer oder der E-Mail Kontakt bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Der zugehörige E-Mail Benutzer oder der zugehörige E-Mail Kontakt wird deaktiviert.
Kontendefinition bei verzögertem Löschen beibehalten	Angabe zur Zuweisung der Kontendefinition bei verzögertem Löschen von Identitäten. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Der E-Mail Benutzer oder der E-Mail Kontakt bleibt erhalten.

Eigenschaft	Beschreibung
	Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Der zugehörige E-Mail Benutzer oder der zugehörige E-Mail Kontakt wird deaktiviert.
Kontendefinition bei Sicherheitsgefährdung beibehalten	Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Identitäten. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Der E-Mail Benutzer oder der E-Mail Kontakt bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Der zugehörige E-Mail Benutzer oder der zugehörige E-Mail Kontakt wird deaktiviert.
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.

Automatisierungsgrade bearbeiten

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

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

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

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.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Automatisierungsgrades.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Automatisierungsgrade auf Seite 70
- Automatisierungsgrade erstellen auf Seite 69
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 69

Automatisierungsgrade erstellen

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

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

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

Um einen Automatisierungsgrad zu erstellen

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

Verwandte Themen

- Stammdaten für Automatisierungsgrade auf Seite 70
- Automatisierungsgrade bearbeiten auf Seite 68
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 69

Automatisierungsgrade an Kontendefinitionen zuweisen

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

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

1. Wählen Sie im Manager die Kategorie **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.

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

   Um eine Zuweisung zu entfernen

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

Stammdaten für Automatisierungsgrade

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 8: Stammdaten eines Automatisierungsgrades

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

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

Abbildungsvorschrift für IT Betriebsdaten erstellen

Eine Kontendefinition legt fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über die primären Rollen einer Identität 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 Identität 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.**
4. Klicken Sie **Hinzufügen** und erfassen Sie folgende Informationen.

- **Spalte**: Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. 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: Die Geschäftsrolle kann nur verwendet werden, wenn das Geschäftsrollenmodul vorhanden ist.
  - keine Angabe

    Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option **Immer Standardwert verwenden** setzen.
- **Standardwert**: Standardwert der Eigenschaft für das Benutzerkonto einer Identität, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann.
- **Immer Standardwert verwenden**: Gibt an, ob die Eigenschaft des Benutzerkontos immer mit dem Standardwert besetzt wird. Es erfolgt keine dynamische Ermittlung der IT Betriebsdaten aus einer Rolle.
- **Benachrichtigung bei Verwendung des Standards**: Gibt an, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage **Identität - Erstellung neues Benutzerkontos mit Standardwerten** verwendet.

5. Speichern Sie die Änderungen.

Verwandte Themen

- IT Betriebsdaten erfassen auf Seite 72

IT Betriebsdaten erfassen

Um für eine Identität 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 Identität wird eine primäre Geschäftsrolle, eine primäre Abteilung, eine primäre Kostenstelle oder ein primärer Standort zugeordnet. Abhängig von dieser Zuordnung werden die gültigen IT Betriebsdaten ermittelt und für die Erstellung des Benutzerkontos verwendet. Können über die primären Rollen keine gültigen IT Betriebsdaten ermittelt werden, werden die Standardwerte verwendet.

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

Beispiel:

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

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

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

Um IT Betriebsdaten festzulegen

1. Wählen Sie im Manager in der Kategorie **Organisationen** oder **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten**.
3. Klicken Sie **Hinzufügen** und erfassen Sie die folgenden Daten.
    - **Wirksam für**: Legen Sie den Anwendungsbereich der IT Betriebsdaten fest. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden.

      Um den Anwendungsbereich festzulegen

        a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.

        b. Wählen Sie unter **Tabelle** die Tabelle, die das Zielsystem abbildet oder, für eine Kontendefinition, die Tabelle `TSBAccountDef`.

        c. Wählen Sie unter **Wirksam für** das konkrete Zielsystem oder die konkrete Kontendefinition.

        d. Klicken Sie **OK**.
    - **Spalte**: Wählen Sie die Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird.

      In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu

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

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

4. Speichern Sie die Änderungen.

Verwandte Themen

- Abbildungsvorschrift für IT Betriebsdaten erstellen auf Seite 71

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

Um die Bildungsregeln auszuführen

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

   - **Alter Wert**: Wert der Objekteigenschaft vor der Änderung der IT Betriebsdaten.

- **Neuer Wert**: Wert der Objekteigenschaft nach der Änderung der IT Betriebsdaten.
- **Auswahl**: Gibt an, ob der neue Wert für das Benutzerkonto übernommen werden soll.

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

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinitionen an Identitäten

Kontendefinitionen werden an die Identitäten des Unternehmens zugewiesen.

Das Standardverfahren für die Zuweisung von Kontendefinitionen an Identitäten ist die indirekte Zuweisung. Die Kontendefinitionen werden an die Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen zugewiesen. Die Identitäten 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 Identitäten zugewiesen werden.

Kontendefinitionen können automatisch an alle Identitäten 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 Identitäten zugewiesen werden oder als Produkte in den IT Shop aufgenommen werden.

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

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

HINWEIS: Solange eine Kontendefinition für eine Identität wirksam ist, behält die Identität ihr daraus entstandenes Benutzerkonto. Wird die Zuweisung einer Kontendefinition entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht. Benutzerkonten, die als **Ausstehend** markiert sind, werden nur gelöscht, wenn der Konfigurationsparameter **QER | Person | User | DeleteOptions | DeleteOutstanding** aktiviert ist.

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Identitäten

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

Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

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

   - ODER -

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

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

Detaillierte Informationen zum Thema

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 76
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 77
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 78
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 79
- Kontendefinitionen an Azure Active Directory Mandanten zuweisen auf Seite 82

Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Kontendefinition an Abteilungen, Kostenstellen oder Standorte zu, damit die Kontendefinitionen über diese Organisationen an Identitäten zugewiesen werden.

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

- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 77
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 77
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 79

Kontendefinitionen an Geschäftsrollen zuweisen

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

Weisen Sie die Kontendefinition an Geschäftsrollen zu, damit die Kontendefinitionen über diese Geschäftsrollen an Identitäten zugewiesen werden.

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. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 76
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 78
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 79

Kontendefinitionen an alle Identitäten zuweisen

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

WICHTIG: Führen Sie die Aufgabe nur aus, wenn sichergestellt ist, dass alle aktuell in der Datenbank vorhandenen internen Identitäten sowie alle zukünftig neu hinzuzufügenden internen Identitäten ein Benutzerkonto in diesem Zielsystem erhalten sollen!

Um eine Kontendefinition an alle Identitäten 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. Wählen Sie die Aufgabe **Automatische Zuweisung zu Identitäten aktivieren**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Speichern Sie die Änderungen.

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

Verwandte Themen

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 76
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 77
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 79

Kontendefinitionen direkt an Identitäten zuweisen

Kontendefinitionen können direkt oder indirekt an Identitäten zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung des Identitäten und der Kontendefinitionen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Kontendefinitionen auch direkt an die Identitäten zuweisen.

Um eine Kontendefinition direkt an Identitäten 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 Identitäten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Identitäten zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 76
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 77
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 78

Kontendefinitionen an Systemrollen zuweisen

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

Mit dieser Aufgabe nehmen Sie eine Kontendefinition in Systemrollen auf.

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.

Kontendefinitionen in den IT Shop aufnehmen

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

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

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

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

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

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

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

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontendefinition an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

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

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

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

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Kontendefinition aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

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

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

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

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

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

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

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

Verwandte Themen

- Stammdaten für Kontendefinitionen auf Seite 66
- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 76
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 77
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 79
- Kontendefinitionen an Systemrollen zuweisen auf Seite 79

Kontendefinitionen an Azure Active Directory Mandanten zuweisen

Wenn Sie die automatische Zuordnung von Benutzerkonten und Identitäten 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 Identität 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 Azure Active Directory 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 Kontendefinitionen an Identitäten auf Seite 75

Kontendefinitionen löschen

Sie können Kontendefinitionen löschen, wenn diese keinem Zielsystem, keiner Identität, 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 Identitäten.
    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. Wählen Sie die Aufgabe **Automatische Zuweisung zu Identitäten deaktivieren**.
    e. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
    f. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Identitäten.
    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 Identitäten zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Identitäten.
    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**.
   d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
   e. 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 Web Designer Web Portal Anwenderhandbuch*.

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

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

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

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

   a. Wählen Sie im Manager die Kategorie **Azure Active Directory > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
   b. Wählen Sie in der Ergebnisliste die Kontendefinition.
   c. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
   d. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
   e. Klicken Sie **OK**.

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

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 Azure Active Directory 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 für Exchange Online

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

Wenn Sie die Berechtigungen 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 Identitäten als Zielsystemadministratoren fest.
2. Die Zielsystemadministratoren nehmen die Identitäten 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 Identitäten als Zielsystemverantwortliche berechtigen und bei Bedarf weitere untergeordnete Anwendungsrollen erstellen und einzelnen Mandanten zuweisen.

Tabelle 9: 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. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Identitäten anlegen, die nicht den Identitätstyp **Primäre Identität** haben. • 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 Identitäten als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Um initial Identitäten 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 **Identitäten zuweisen**.
4. Weisen Sie die Identität zu und speichern Sie die Änderung.

Um initial Identitäten 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 **Identitäten zuweisen**.
4. Weisen Sie die Identitäten zu und speichern Sie die Änderungen.

Um als Zielsystemverantwortlicher weitere Identitäten 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 **Identitäten zuweisen**.
4. Weisen Sie die Identitäten 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 Identitäten 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 11

Jobserver für Exchange Online-spezifische Prozessverarbeitung

Für die Verarbeitung der Exchange Online spezifischen Prozesse im One Identity Manager müssen die Server mit ihren Serverfunktionen bekannt sein. Dazu gehört beispielsweise der Synchronisationsserver.

Um die Funktion eines Servers zu definieren, haben Sie mehrere Möglichkeiten:

- Erstellen Sie im Designer in der Kategorie **Basisdaten > Installationen > Jobserver** einen Eintrag für den Jobserver. Ausführliche Informationen dazu finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Wählen Sie im Manager in der Kategorie **Azure Active Directory > Basisdaten zur Konfiguration > Server** einen Eintrag für den Jobserver und bearbeiten Sie die Stammdaten des Jobservers.

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

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

Um einen Jobserver und seine Funktionen zu bearbeiten

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Jobserver auf Seite 88
- Festlegen der Serverfunktionen auf Seite 91

Allgemeine Stammdaten für Jobserver

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

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

Tabelle 10: Eigenschaften eines Jobservers

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS-Syntax. Syntax: `<Name des Servers>.<Vollqualifizierter Domänenname>`
Zielsystem	Zielsystem des Computerkontos.
Sprache	Sprache des Servers.
Server ist Cluster	Gibt an, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. HINWEIS: Die Eigenschaften **Server ist Cluster** und **Server gehört zu Cluster** schließen einander aus.
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.
IP-Adresse (IPv4)	Internet Protokoll Version 4 (IPv4)-Adresse des Servers.
Kopierverfahren (Quellserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Quelle einer Kopieraktion ist. Derzeit werden nur Kopierverfahren über die Programme `Robocopy` und `rsync` unterstützt. Wird kein Verfahren angegeben, ermittelt der One Identity Manager Service zur Laufzeit das Betriebssystem des Servers, auf dem die Kopieraktion ausgeführt wird. Die Replikation erfolgt dann zwischen Servern mit einem Windows Betriebssystem mit dem Programm `Robocopy` und zwischen Servern mit einem Linux Betriebssystem mit dem Programm `rsync`. Unterscheiden sich die Betriebssysteme des Quellservers und des Zielservers, so ist für eine erfolgreiche Replikation die Angabe der zulässigen Kopierverfahren zwingend erforderlich. Es wird das Kopierverfahren eingesetzt, das beide Server unterstützen.
Codierung	Codierung des Zeichensatzes mit der Dateien auf dem Server geschrieben werden.
Übergeordneter Jobserver	Bezeichnung des übergeordneten Jobservers.

Eigenschaft	Bedeutung
Ausführender Server	Bezeichnung des ausführenden Servers. Eingetragen wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden. Diese Angabe wird bei der automatischen Aktualisierung des One Identity Manager Service ausgewertet. Verarbeitet ein Server mehrere Queues, wird mit der Auslieferung von Prozessschritten solange gewartet, bis alle Queues, die auf demselben Server abgearbeitet werden, die automatische Aktualisierung abgeschlossen haben.
Queue	Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Mit dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Serverbetriebssystem	Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte **Win32**, **Windows**, **Linux** und **Unix**. Ist die Angabe leer, wird **Win32** angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen.
One Identity Manager Service installiert	Gibt an, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur `QBM_PJobQueueLoad` aktiviert, sobald die Queue das erste Mal angefragt wird. Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.
Stopp One Identity Manager Service	Gibt an, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten.

Eigenschaft	Bedeutung
	Den Dienst können Sie mit entsprechenden administrativen Berechtigungen im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*.
Pausiert wegen Nichtverfügbarkeit eines Zielsystems	Gibt an, ob die Verarbeitung von Aufträgen für diese Queue angehalten wurde, weil das Zielsystem, für den dieser Jobserver der Synchronisationsserver ist, vorübergehend nicht erreichbar ist. Sobald das Zielsystem wieder erreichbar ist, wird die Verarbeitung gestartet und alle anstehenden Aufträge werden ausgeführt. Ausführliche Informationen zum Offline-Modus finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.
Kein automatisches Softwareupdate	Gibt an, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.
Softwareupdate läuft	Gibt an, ob gerade eine Softwareaktualisierung ausgeführt wird.
Serverfunktion	Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

Verwandte Themen

- Festlegen der Serverfunktionen auf Seite 91

Festlegen der Serverfunktionen

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

Die Serverfunktion definiert die Funktion eines Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

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

Tabelle 11: Zulässige Serverfunktionen

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

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

Verwandte Themen

- Allgemeine Stammdaten für Jobserver auf Seite 88

Exchange Online Organisationskonfiguration

Die Exchange Online Organisationskonfigurationen der Azure Active Directory Mandanten werden in die One Identity Manager-Datenbank eingelesen. Aufgrund der komplexen Zusammenhänge und weitreichenden Auswirkungen von Änderungen ist die Anpassung dieser Informationen im One Identity Manager nicht möglich.

Detaillierte Informationen zum Thema

Erweiterungen für Azure Active Directory Mandanten

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

Am Azure Active Directory Mandanten werden für Exchange Online folgende zusätzliche Informationen abgebildet.

- Initiale Kontendefinitionen für die Erzeugung von E-Mail Kontakten (**E-Mail Kontendefinition (initial)**) oder E-Mail Benutzern (**E-Mail Benutzerdefinition (initial)**)

  Diese Kontendefinitionen werden verwendet, wenn für diesen Azure Active Directory Mandanten die automatische Zuordnung von Identitäten zu Benutzerkonten genutzt wird und dabei bereits verwaltete E-Mail Kontakte oder E-Mail Benutzer (Zustand

Linked configured) entstehen sollen. Es wird der Standardautomatisierungsgrad der Kontendefinition angewendet.

- **Zielsystemverantwortliche (Exchange Online)**: Anwendungsrolle, in der die Exchange Online Zielsystemverantwortlichen für die des Azure Active Directory Mandanten festgelegt sind. Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Exchange Online** oder einer untergeordneten Anwendungsrolle zugewiesen sein.
- Erweiterungen für die Vererbung von Berechtigungen über Kategorien

  Für Exchange Online kann die Vererbung von Office 365 Gruppen und E-Mail-aktivierten Verteilergruppen über Kategorien genutzt werden.

Um die Stammdaten eines Azure Active Directory Mandanten zu bearbeiten

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

Verwandte Themen

- Kontendefinitionen an Azure Active Directory Mandanten zuweisen auf Seite 82
- Zielsystemverantwortliche für Exchange Online auf Seite 85
- Vererbung von Exchange Online E-Mail-aktivierten Verteilergruppen anhand von Kategorien auf Seite 167
- Vererbung von Exchange Online Office 365 Gruppen anhand von Kategorien auf Seite 191

Hierarchische Adressbücher anzeigen

In einem hierarchischen Adressbuch (HAB) werden die Empfänger (Postfächer, E-Mail Benutzer, E-Mail Kontakte, E-Mail-aktivierte Verteilergruppen) in einer hierarchischen Organisationsstruktur dargestellt.

Ausführliche Informationen finden Sie unter https://learn.microsoft.com/en-us/exchange/address-books/hierarchical-address-books/hierarchical-address-books.

Der Aufbau der hierarchische Struktur erfolgt über die Hierarchie der Azure Active Directory Gruppen. Die Azure Active Directory Gruppe, welche die Basis des hierarchischen Adressbuchs darstellt, ist mit der Exchange Online Organisation verknüpft. Die E-Mail-aktivierte Verteilergruppen, die ein hierarchisches Adressbuch abbilden, werden mit der Option **Hierarchische Gruppe** gekennzeichnet.

Für die Sortierung der Empfänger für die Anzeige werden die folgenden Eigenschaften verwendet.

- **Reihenfolge**: Gibt an, in welcher Reihenfolge die Empfänger im hierarchischen Adressbuch angezeigt werden. Je größer der Wert desto höher die Rangfolge in der Sortierung.
- **Phonetischer Anzeigename**: Ist keine Reihenfolge angegeben oder haben mehrere Einträge die gleiche Reihenfolge, erfolgt die Sortierung nach dem phonetischen Anzeigenamen.
- **Anzeigename**: Ist kein phonetischer Anzeigenamen eingetragen, erfolgt die Sortierung nach dem Anzeigenamen.

Um das hierarchische Adressbuch anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten**.
2. Wählen Sie in der Ergebnisliste den Azure Active Directory Mandanten.
3. Wählen Sie den Bericht **Hierarchisches Adressbuch anzeigen**.

Verwandte Themen

- Stammdaten für Exchange Online E-Mail-aktivierte Verteilergruppen auf Seite 146
- Allgemeine Stammdaten für Exchange Online Postfächer auf Seite 102
- Stammdaten für Exchange Online E-Mail Benutzer auf Seite 121
- Stammdaten für Exchange Online E-Mail Kontakte auf Seite 134

Exchange Online Öffentliche Ordner

Öffentliche Ordner werden eingesetzt, um den Identitäten den gemeinsamen Zugriff auf Informationen zu ermöglichen. Öffentliche Ordner können hierarchisch aufgebaut sein und sind mit einer Datenbank für öffentliche Ordner verbunden.

Exchange Online öffentliche Ordner werden durch die Synchronisation in den One Identity Manager eingelesen und können im One Identity Manager nicht bearbeitet werden.

Um Informationen zu einem öffentlichen Ordner anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten > <Azure Active Directory Mandant> > Exchange Online Administration > Organisationskonfiguration > Öffentliche Ordner**.
2. Wählen Sie in der Ergebnisliste den öffentlichen Ordner.
3. Wählen Sie eine der folgenden Aufgaben:
    - **Überblick über den Exchange Online öffentlichen Ordner**: Sie erhalten einen Überblick über den öffentlichen Ordner und seine Abhängigkeiten.

- **Stammdaten anzeigen**: Es werden die Stammdaten für den öffentlichen Ordner angezeigt.

Verwandte Themen

- Exchange Online E-Mail-aktivierte öffentliche Ordner auf Seite 202
- Einzelobjekte synchronisieren auf Seite 53

Exchange Online Richtlinien

Exchange Online Richtlinien werden durch die Synchronisation in den One Identity Manager eingelesen und können im One Identity Manager nicht bearbeitet werden. Sie können die Richtlinien an Exchange Online Postfächer zuweisen.

Richtlinien für Freigabeverwaltung

Richtlinien für Freigaben werden eingesetzt, um externen Benutzern Kalenderinformationen und Kontaktdaten zur Verfügung zu stellen. Mit der Zuweisung einer Freigaberichtlinie an ein Postfach wird geregelt, wie dieses Kalenderinformationen und Kontaktdaten für Benutzer außerhalb der Exchange Online Organisation freigeben kann.

Aufbewahrungsrichtlinien

Aufbewahrungsrichtlinien werden eingesetzt, um Einstellungen für die Aufbewahrung von Ordnern und E-Mail Benachrichtigungen zusammenzufassen und auf Postfächer anzuwenden.

Outlook Web App Postfachrichtlinien

Outlook Web App Postfachrichtlinien werden eingesetzt, um den Zugriff auf Funktionen in Outlook Web App zu verwalten.

Postfachrichtlinien für mobile Geräte

Postfachrichtlinien für die mobile E-Mail Abfrage enthalten Einstellungen, die beim Zugriff auf die Daten mit mobilen Geräten über das Synchronisationsprotokoll Exchange ActiveSync wirksam werden. Die Einstellungen umfassen beispielsweise Kennwortanforderungen, Festlegungen für E-Mail Anlagen, Angaben zur Geräteverschlüsselung und Zugriffsregelungen auf Dateifreigaben.

Rollenzuweisungsrichtlinien

Richtlinien für Rollenzuweisungen werden eingesetzt, um Benutzern Funktionen und Aufgaben für die Verwaltung ihrer Postfächer zur Verfügung zu stellen.

Um Informationen zu einer Richtlinie anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten > <Azure Active Directory Mandant> > Exchange Online Administration > Richtlinien > <Art der Richtlinie>**.
2. Wählen Sie in der Ergebnisliste die Richtlinie.
3. Wählen Sie eine der folgenden Aufgaben:
   - **Überblick über die Exchange Online Richtlinie**: Sie erhalten einen Überblick über die Richtlinie und ihre Abhängigkeiten.
   - **Stammdaten anzeigen**: Es werden die Stammdaten für die Richtlinie angezeigt.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 53
- Richtlinien und Funktionen für Exchange Online Postfächer auf Seite 107

Exchange Online Postfächer

Exchange Online Postfächer können Nachrichten senden, empfangen und speichern. Exchange Online kennt verschiedene Postfachtypen. Nachfolgend sind die im One Identity Manager unterstützten Typen von Postfächern aufgeführt. Exchange Online Postfächer werden durch die Synchronisation in den One Identity Manager eingelesen.

Tabelle 12: Unterstützte Postfachtypen

Postfachtyp	Beschreibung
Benutzerpostfach	Benutzerpostfächer werden den Azure Active Directory Benutzerkonten in einer Exchange Online Organisation zugeordnet. Benutzerpostfächer können Sie nicht im One Identity Manager erstellen. Benutzerpostfächer werden erzeugt, indem den Azure Active Directory Benutzerkonten entsprechende Abonnements zugewiesen werden. Dadurch entstehen Benutzerpostfächer, die erst nach Synchronisation in der One Identity Manager-Datenbank erscheinen. Danach können die Benutzerpostfächer automatisch in Exchange Online provisioniert werden
Gerätepostfach	Gerätepostfächer sind Ressourcenpostfächer, die zur Planung von Ressourcen, wie beispielsweise Computer oder Laptops verwendet werden. Gerätepostfächer können Sie im One Identity Manager erstellen. Beim Erzeugen eines Gerätepostfachs wird zusätzlich ein Azure Active Directory Benutzerkonto erzeugt und mit dem Postfach verknüpft.
Raumpostfach	Raumpostfächer sind Ressourcenpostfächer, die zur Planung von Besprechungsorten verwendet werden. Raumpostfächer können Sie im One Identity Manager erstellen. Beim Erzeugen eines Raumpostfachs wird zusätzlich ein Azure Active Directory Benutzerkonto erzeugt und mit dem Postfach verknüpft.
Freigegebenes Postfach	Freigegebene Postfächer sind Postfächer, die von mehreren Benutzern verwendet werden.

Postfachtyp	Beschreibung
	Freigegebene Postfächer können Sie im One Identity Manager erstellen. Beim Erzeugen eines freigegebenen Postfachs wird zusätzlich ein Azure Active Directory Benutzerkonto erzeugt und mit dem Postfach verknüpft.
Discovery-Postfach	Im Exchange Online wird standardmäßig ein Discovery-Postfach erstellt, welches als Zielpostfach für Suchen mittels eDiscovery eingesetzt wird. Discovery-Postfächer sind im One Identity Manager nicht bearbeitbar.

Detaillierte Informationen zum Thema

- Exchange Online Postfächer erstellen auf Seite 100
- Stammdaten für Exchange Online Postfächer bearbeiten auf Seite 101
- Allgemeine Stammdaten für Exchange Online Postfächer auf Seite 102
- Grenzwerte und Nutzung für Exchange Online Postfächer auf Seite 105
- Richtlinien und Funktionen für Exchange Online Postfächer auf Seite 107
- Buchung von Ressourcen für Exchange Online Gerätepostfächer und Exchange Online Raumpostfächer auf Seite 109
- Empfangsbeschränkungen für Exchange Online Postfächer anpassen auf Seite 113
- Exchange Online Postfachberechtigung: Senden im Auftrag auf Seite 114
- Exchange Online Postfachberechtigung: Senden als auf Seite 115
- Exchange Online Postfachberechtigung: Vollzugriff auf Seite 116
- Moderatoren für Exchange Online Postfächer festlegen auf Seite 116
- Zusatzeigenschaften an Exchange Online Postfächer zuweisen auf Seite 117
- Exchange Online Postfächer löschen auf Seite 118
- Einzelobjekte synchronisieren auf Seite 53

Exchange Online Postfächer erstellen

Exchange Online Postfächer werden durch die Synchronisation in den One Identity Manager eingelesen.

Benutzerpostfächer können Sie nicht im One Identity Manager erstellen. Benutzerpostfächer werden erzeugt, indem den Azure Active Directory Benutzerkonten entsprechende Abonnements zugewiesen werden. Dadurch entstehen Benutzerpostfächer, die erst nach Synchronisation in der One Identity Manager-Datenbank erscheinen. Danach können die Benutzerpostfächer automatisch in Exchange Online provisioniert werden.

Gerätepostfächer, Raumpostfächer und freigegebene Postfächer können Sie im One Identity Manager erstellen. Beim Erzeugen eines Gerätepostfachs, Raumpostfachs

oder freigegebenen Postfachs wird zusätzlich ein Azure Active Directory Benutzerkonto erzeugt und mit dem Postfach verknüpft.

Um ein Postfach zu erstellen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Postfächer**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular erfassen Sie die Stammdaten des Postfachs.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für Exchange Online Postfächer auf Seite 102
- Grenzwerte und Nutzung für Exchange Online Postfächer auf Seite 105
- Richtlinien und Funktionen für Exchange Online Postfächer auf Seite 107
- Buchung von Ressourcen für Exchange Online Gerätepostfächer und Exchange Online Raumpostfächer auf Seite 109
- Stammdaten für Exchange Online Postfächer bearbeiten auf Seite 101

Stammdaten für Exchange Online Postfächer bearbeiten

Um ein Postfach zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Postfächer**.
2. Wählen Sie in der Ergebnisliste das Postfach und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten des Postfachs.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für Exchange Online Postfächer auf Seite 102
- Grenzwerte und Nutzung für Exchange Online Postfächer auf Seite 105
- Richtlinien und Funktionen für Exchange Online Postfächer auf Seite 107
- Buchung von Ressourcen für Exchange Online Gerätepostfächer und Exchange Online Raumpostfächer auf Seite 109
- Exchange Online Postfächer erstellen auf Seite 100

Allgemeine Stammdaten für Exchange Online Postfächer

Erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 13: Allgemeine Stammdaten eines Postfachs

Eigenschaft	Beschreibung
Identität	Identität, die das Postfach verwendet.
Keine Verbindung mit einer Identität erforderlich	Gibt an, ob dem Postfach absichtlich keine Identität zugeordnet ist. Der Wert wird aus dem verbundenen Benutzerkonto ermittelt.
Nicht mit einer Identität verbunden	Zeigt an, warum für das Postfach die Option **Keine Verbindung mit einer Identität erforderlich** aktiviert ist. Der Wert wird aus dem verbundenen Benutzerkonto ermittelt. Mögliche Werte sind: • **durch Administrator**: Die Option wurde manuell durch den Administrator aktiviert. • **durch Attestierung**: Das Benutzerkonto wurde attestiert. • **durch Ausschlusskriterium**: Das Benutzerkonto wird aufgrund eines Ausschlusskriteriums nicht mit einer Identität verbunden. Das Benutzerkonto ist beispielsweise in der Ausschlussliste für die automatische Identitätenzuordnung enthalten (Konfigurationsparameter **PersonExcludeList**).
Azure Active Directory Mandant	Bezeichnung des Azure Active Directory Mandanten.
Azure Active Directory Benutzerkonto	Azure Active Directory Benutzerkonto, welches das Postfach verwendet.
Bezeichnung	Bezeichnung des Postfachs.
Anzeigename	Anzeigename, wie er im Adressbuch verwendet wird.
Einfache Anzeige	Einfacher Anzeigename für Systeme, die nicht alle Zeichen des normalen Anzeigenamens interpretieren können.
Phonetischer Anzeigename	Anzeigename in phonetischer Schreibweise. Wird verwendet, wenn die Aussprache und Schreibweise des Namens nicht übereinstimmen. Der phonetische Anzeigename wird beispielsweise verwendet, um die Empfänger im hierarchischen Adressbuch zu sortieren, wenn keine Reihenfolge angegeben ist. Die Sortierung erfolgt aufsteigend von A bis Z.

Eigenschaft	Beschreibung
	Ist kein phonetischer Anzeigenamen eingetragen, erfolgt die Sortierung nach dem Anzeigenamen.
Reihenfolge	Gibt an, in welcher Reihenfolge die Empfänger im hierarchischen Adressbuch angezeigt werden. Je größer der Wert desto höher die Rangfolge in der Sortierung. Ist keine Reihenfolge angegeben oder haben mehrere Einträge die gleiche Reihenfolge, erfolgt die Sortierung nach dem phonetischen Anzeigenamen.

Benutzer-ID	Benutzer-ID, mit der sich der Benutzer am Postfach anmeldet.
	Beispiel:
	`<alias>@<domain.com>`
	`<user>@yourorganisation.onmicrosoft.com`

Alias	Eindeutiger E-Mail Alias zur Identifizierung des Postfaches.
Proxy Adressen	E-Mail-Adressen zum Postfach. Als Adresstyp können Sie zusätzlich zur Standardadressierung (SMTP, X400) weitere Mailkonnektoren (beispielsweise CCMail, MS) nutzen. Für die Erstellung weiterer Proxyadressen ist die folgende Syntax einzuhalten: `Adresstyp: neue E-Mail-Adresse`
Empfängertyp (Detail)	Typ des Postfachs. Zur Auswahl stehen **Benutzerpostfach**, **Raumpostfach**, **Gerätepostfach**, **Freigegebenes Postfach** und **Discovery-Postfach**.
Nicht in Adresslisten anzeigen	Gibt an, ob das Postfach in Adressbüchern angezeigt werden soll. Setzen Sie die Option, wenn Sie verhindern wollen, dass das Postfach in Adressbüchern angezeigt wird. Diese Option gilt für die Anzeige in allen Adressbüchern.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten Gruppen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen an das Postfach. Gruppen können selektiv an die Postfächer vererbt werden. Dazu werden die Gruppen und die Postfächer in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Gruppen erbbar	Gibt an, ob das Postfach Gruppen über die Identität erben darf.

Eigenschaft	Beschreibung
	Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an das Postfach vererbt. • Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Postfach diese Gruppen. • Wenn eine Identität eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Postfach diese Gruppe nur, wenn die Option aktiviert ist.
Übermitteln und Weiterleiten	Gibt an, ob Nachrichten übermittelt und weitergeleitet werden dürfen. Aktivieren Sie diese Option, um die Nachrichten an den alternativen Empfänger und den Postfachbesitzer zu senden.
Alternative Empfänger	Alternativer Empfänger, an welche die Nachrichten für dieses Postfach weitergeleitet werden sollen. Sie können entweder einen alternativen Empfänger, eine Empfängergruppe oder einen Empfangsordner angeben. ***Um einen alternativen Empfänger festzulegen*** 1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. 2. Wählen Sie unter **Tabelle** die Tabelle, die die Empfänger abbildet. 3. Wählen Sie unter **Alternative Empfänger** den Empfänger. 4. Klicken Sie **OK**.
Absender-Authentifizierung anfordern	Gibt an, ob die Authentifizierungsinformationen von Absendern angefordert werden. Setzen Sie die Option, um zu verhindern, dass anonyme Absender Benachrichtigungen an das Postfach senden können.
Moderation aktiviert	Gibt an, ob das Postfach moderiert wird. Legen Sie die Moderatoren über die Aufgabe **Moderatoren zuweisen** fest. Anschließend aktivieren Sie die Option.
Senden der Benachrichtigung	Angabe, wie Absender benachrichtigt werden, wenn Sie ein Nachricht an ein moderiertes Postfach senden. Zulässige Werte sind: • **Keine Benachrichtigung**: Es erfolgt keine Benachrichtigung der Absender.

Eigenschaft	Beschreibung
	• **Nur Absender der eigenen Organisation benachrichtigen**: Nur interne Absender erhalten eine Benachrichtigung. • **Alle Absender benachrichtigen**: Interne und externe Absender erhalten eine Benachrichtigung.
Lesestatusverfolgung aktiviert	Gibt an, ob dieses Postfach den Lesestatus gesendeter Nachrichten anzeigen kann.

Verwandte Themen

- Moderatoren für Exchange Online Postfächer festlegen auf Seite 116
- Zuweisen von Exchange Online E-Mail-aktivierten Verteilergruppen an Exchange Online Empfänger auf Seite 153

Grenzwerte und Nutzung für Exchange Online Postfächer

Auf dem Tabreiter **Postfachnutzung** werden folgende Informationen abgebildet.

Tabelle 14: Grenzwerte für ein Postfach

Eigenschaft	Beschreibung
Letzte Anmeldung	Zeitpunkt der letzte Anmeldung am Postfach.Diese Angabe wird durch die Synchronisation ermittelt und ist nicht bearbeitbar.
Letzte Abmeldung	Zeitpunkt der letzte Abmeldung am Postfach.Diese Angabe wird durch die Synchronisation ermittelt und ist nicht bearbeitbar.
Letztes angemeldetes Benutzerkonto	Name des Benutzerkontos, mit dem die letzte Anmeldung am Postfach erfolgte. Diese Angabe wird durch die Synchronisation ermittelt und ist nicht bearbeitbar.
Status Speichergrenze	Kennzeichnet den Füllstand des Postfachs gegenüber den festgelegten Grenzwerten. Diese Angabe wird durch die Synchronisation ermittelt und ist nicht bearbeitbar.
Anzahl der gespeicherten Nachrichten	Anzahl der gespeicherten Nachrichten in diesem Postfach. Diese Angabe wird durch die Synchronisation ermittelt und ist nicht bearbeitbar.
Anzahl zugeordneter Elemente	Anzahl zugeordneter Elemente in diesem Postfach.Diese Angabe wird durch die Synchronisation ermittelt und ist nicht bearbeitbar.

Eigenschaft	Beschreibung
Belegter Speicherplatz [Byte]	Belegter Speicherplatz in Byte. Diese Angabe wird durch die Synchronisation ermittelt und ist nicht bearbeitbar.
Anzahl wiederherstellbarer Elemente	Anzahl an Nachrichten im Ordner **Wiederherstellbare Elemente**. Diese Angabe wird durch die Synchronisation ermittelt und ist nicht bearbeitbar.
Größe wiederherstellbarer Elemente	Größe der Nachrichten im Ordner **Wiederherstellbare Elemente**. Diese Angabe wird durch die Synchronisation ermittelt und ist nicht bearbeitbar.
Standardwerte der Datenbank benutzen	Gibt an, ob die Grenzwerte des Postfachdatenbank zu verwenden sind. Diese Angabe wird durch die Synchronisation ermittelt und ist nicht bearbeitbar. Option aktiviert: Die Grenzwerte des Postfachdatenbank werden verwendet. Option nicht aktiviert: Die Grenzwerte des Postfachs werden verwendet.
Max. wiederherstellbare Elemente	Maximale Anzahl an Nachrichten, die ein Ordner im Ordner **Wiederherstellbare Elemente** enthalten darf. Diese Angabe wird durch die Synchronisation ermittelt und ist nicht bearbeitbar.
Warnen ab [Wiederherstellbare Elemente]	Anzahl der Elemente, die ein Ordner im Ordner **Wiederherstellbare Elemente** enthalten darf, bevor der Benutzer eine Warnung erhält. Diese Angabe wird durch die Synchronisation ermittelt und ist nicht bearbeitbar.
Gelöschte Objekte aufbewahren [Tage]	Anzahl der Tage, die gelöschte Objekte (beispielsweise E-Mail Nachrichten) auf dem Server verbleiben, bevor sie endgültig entfernt werden.
Größe von Regeln [KB]	Grenzwert für die Größe von Regeln.
Transfer verbieten ab [KB]	Größe der Postfächer in KB, ab der das Senden und Empfangen von Nachrichten verboten ist.
Senden verbieten ab [KB]	Größe der Postfächer in KB, ab der das Senden von Nachrichten verboten ist. Bei Überschreitung dieser Größe erhält der Benutzer eine Nachricht, dass Nachrichten in seinem Postfach gelöscht werden müssen. Der Benutzer ist nicht in der Lage weitere Nachrichten zu versenden bis die Größe seines Postfaches reduziert wurde.
Warnen ab [KB]	Maximale Größe der Postfächer in KB. Bei Überschreitung dieser Größe erhält der Benutzer eine Warnung, dass Nachrichten in seinem Postfach gelöscht werden müssen.

Richtlinien und Funktionen für Exchange Online Postfächer

Auf dem Tabreiter **Funktionen** erfassen Sie die folgenden Stammdaten.

Tabelle 15: Funktionen für ein Postfach

Eigenschaft	Beschreibung
Freigaberichtlinie	Freigaberichtlinie, die für dieses Postfach gelten soll.
Rollenzuweisungsrichtlinie	Rollenzuweisungsrichtlinie, die für dieses Postfach gelten soll.
Postfachrichtlinien für mobile Geräte	Postfachrichtlinien für mobile Geräte, die für dieses Postfach gelten soll.
Outlook Web App Postfach-richtlinie	Outlook Web App Postfachrichtlinie, die für dieses Postfach gelten soll.
Aufbewahrungsrichtlinie	Aufbewahrungsrichtlinie aus, die für dieses Postfach gelten soll.
Outlook Web App aktiviert	Gibt an, ob die Funktion für Microsoft Office Outlook Web App aktiviert ist. Office Outlook Web App ermöglicht den Postfachzugriff über Webbrowser.
Mobiler Zugang	Gibt an, ob auf mobilen Geräten der Zugriff auf das Postfach möglich ist.
Exchange Webdienste aktiviert	Gibt an, ob für das Postfach der Zugriff über Exchange-Webdienste aktiviert ist.
IMAP4 aktiviert	Gibt an, ob die Funktion für IMAP4 Zugriff aktiviert ist.
POP3 aktiviert	Gibt an, ob die Funktion für POP3 Zugriff aktiviert ist.
MAPI aktiviert	Gibt an, ob die Funktion für MAPI Zugriff aktiviert ist. MAPI ermöglicht den Postfachzugriff über einen MAPI-Client, beispielsweise Outlook.
Kalenderreparatur deaktiviert	Gibt an, ob verhindert werden soll, dass Kalenderelemente im Postfach vom Kalenderreparatur-Assistenten repariert werden.
Kalenderversionierung deakti-viert	Gibt an, ob verhindert werden soll, dass Kalenderänderungen im Postfach erfasst werden.
Archivierung aktiviert	Gibt an, ob ein persönliches Archiv für dieses Postfach erzeugt werden soll. Um ein persönliches Archiv für ein Postfach einzurichten, aktivieren Sie die Option.

Eigenschaft	Beschreibung
Name des Archivs	Bezeichnung des Archivs.
Aufbewahrungspflicht	Gibt an, ob die Aufbewahrung des Postfaches erforderlich ist.
Aufbewahrung aktiviert von	Benutzer, der für das Postfach die Aufbewahrungspflicht aktiviert hat.
Aufbewahrungsdatum	Datum, ab dem das Postfach der Aufbewahrungspflicht unterliegt.
Kommentar zur Aufbewahrungspflicht	Zusätzlicher Kommentar, um die Benutzer zu informieren, wenn die Option **Aufbewahrungspflicht** aktiviert wird. Diese Angabe wird dem Benutzer im Outlook angezeigt.
Website zur Aufbewahrungspflicht	Webseite oder ein Dokument mit weiteren Informationen, um die Benutzer zu informieren, wenn die Option **Aufbewahrungspflicht** aktiviert wird. Diese Angabe wird dem Benutzer im Outlook angezeigt.
Anhalten der Aufbewahrungsrichtlinie im Zeitraum	Gibt an, ob die Aufbewahrungsrichtlinie temporär angehalten werden soll. Setzen Sie die Option, wenn die Richtlinien zur Aufbewahrungszeit für ein Postfach vorübergehend ausgesetzt werden sollen, beispielsweise für Urlaubszeiten. Den Zeitraum legen Sie über die Eingaben **Startdatum** und **Enddatum** fest.
Startdatum	Startdatum zum Anhalten der Aufbewahrungsrichtlinie.
Enddatum	Enddatum zum Anhalten der Aufbewahrungsrichtlinie.
Überwachungsprotokollierung aktiviert	Gibt an, ob die Postfach-Überwachungsprotokollierung für das Postfach aktiviert oder deaktiviert sein soll.
Administratoraktionen aufzeichnen	Angabe der Postfachvorgänge, die für Administratoren als Teil der Postfach-Überwachungsprotokollierung erfasst werden. Ausführliche Informationen zu Postfachüberwachungsprotokollierung und zu den aufzuzeichnenden Postfachaktionen finden Sie in der Dokumentation von Microsoft.
Stellvertreteraktionen aufzeichnen	Angabe der Postfachvorgänge, die für Stellvertretungsbenutzer als Teil der Postfach-Überwachungsprotokollierung erfasst werden.

Eigenschaft	Beschreibung
	Ausführliche Informationen zu Postfachüberwachungsprotokollierung und zu den aufzuzeichnenden Postfachaktionen finden Sie in der Dokumentation von Microsoft.
Eigentümeraktionen aufzeichnen	Angabe der Postfachvorgänge, um die Postfachbesitzer als Teil der Postfach-Überwachungsprotokollierung zu erfassen. Ausführliche Informationen zu Postfachüberwachungsprotokollierung und zu den aufzuzeichnenden Postfachaktionen finden Sie in der Dokumentation von Microsoft.
Überwachungsprotokolleinträge aufbewahren [Tage]	Maximales Alter für Überwachungsprotokolleinträge in einem Postfach. Protokolleinträge, die älter sind als der angegebene Wert, werden entfernt.

Verwandte Themen

- Exchange Online Richtlinien auf Seite 97

Buchung von Ressourcen für Exchange Online Gerätepostfächer und Exchange Online Raumpostfächer

Für Gerätepostfächer und Raumpostfächer können Sie die Buchung und Planung von Ressourcen konfigurieren.

Auf dem Tabreiter **Buchungsoptionen** erfassen Sie die folgenden Stammdaten.

Tabelle 16: Stammdaten zur Buchung von Ressourcen

Eigenschaft	Beschreibung
Kapazität für Ressourcen	Kapazität der Ressource, beispielsweise die Anzahl der Sitzplätze in einem Besprechungsraum.
Kalenderautomatik aktiviert	Gibt an, ob bei Gerätepostfächer und Raumpostfächer die Ressourcenbuchungsautomatik aktiviert ist, damit Buchungsanfragen automatisch verarbeitet werden können. Zulässige Werte sind: • **Kalenderautomatik deaktiviert**: Die

Eigenschaft	Beschreibung
	Kalenderautomatik ist nicht aktiviert. • **Kalenderautomatik aktiviert**: Die Kalenderautomatik ist aktiviert. • **Ressourcenbuchungsautomatik aktiviert**: Bei Postfächern vom Typ **Raumpostfach** ist der automatische Buchungsassistent aktiviert.
Wiederkehrende Buchung erlauben	Gibt an, ob Serien von Buchungen zulässig sind.
Buchung nur für Arbeitszeit möglich	Gibt an, ob die Ressource nur innerhalb der Arbeitszeit oder auch außerhalb der Arbeitszeit gebucht werden kann.
Wiederkehrende Buchungen nach max. Planungszeitraum abweisen	Gibt an, ob Buchungsserien über den maximal zulässigen Planungszeitraum hinaus, erstellt werden können.
Max. Planungszeitraum [Tage]	Maximaler Planungszeitraum für Buchungsanfragen in Tagen.
Max. Dauer [Min]	Maximal zulässige Buchungsdauer einer Ressource in Minuten.
Buchungsberechtigung für alle	Gibt an, ob richtlinienkonforme Buchungsanfragen von allen Benutzern automatisch genehmigt werden. Ist die Option deaktiviert, legen Sie über die Aufgabe **Buchungsberechtigung zuweisen** einzelne Benutzer fest, die richtlinienkonforme Anfragen senden dürfen, die automatisch genehmigt werden.
Buchungsanfragenberechtigung für alle	Gibt an, ob alle Benutzer Buchungsanfragen, die den Richtlinien entsprechen, senden dürfen. Ist die Option deaktiviert, legen Sie über die Aufgabe **Richtlinienkonforme Buchungsanfragen erlauben** einzelne Benutzer fest, die Buchungsanfragen senden dürfen, die den Richtlinien entsprechen.
Richtlinienunabhängige Buchungsanfragenberechtigung für alle	Gibt an, ob alle Benutzer Buchungsanfragen, die nicht den Richtlinien genügen, senden dürfen. Ist die Option deaktiviert, legen Sie über die Aufgabe **Richtlinienunabhängige Buchungsanfragen erlauben** einzelne Benutzer fest, die Buchungsanfragen senden dürfen, die nicht den Richtlinien entsprechen.

Eigenschaft	Beschreibung
Konflikte erlauben	Gibt an, ob Buchungsanfragen, die sich überschneiden, zulässig sind.
Max. Konflikte für Serien [%]	Schwellwert in Prozent für die zulässigen Konflikte bei Überschneidung einer Buchungsserien mit anderen Buchungen. Wird dieser Wert überschritten, wird die Serienanfrage abgelehnt.
Max. Anzahl Konflikte für Serien	Maximale Anzahl von Konflikten, die für die Überschneidung von Buchungsserien mit anderen Buchungen zulässig sind. Wird der Wert überschritten, wird die Serienanfrage abgelehnt.
Buchungsanfrage weiterleiten	Gibt an, ob Buchungsanfragen an die Stellvertreter des Ressourcenpostfachs weitergeleitet werden. Die Stellvertreter entscheiden über die Buchungsanfragen.
Terminanfragen von externen Absendern zulassen	Gibt an, ob externe Absender Terminanfragen in den Kalender eintragen können.
Name des Organisators an Betreff anhängen	Gibt an, ob der Name des Organisators im Betreff der Buchungsanfrage angegeben wird.
Organisator über abgelehnte Buchung informieren	Gibt an, ob der Organisator informiert wird, wenn eine Buchungsanfrage aufgrund von Konflikten abgelehnt wird.
Zusatzinformation zu abgelehnter Buchung senden	Gibt an, ob zusätzliche Informationen als Antwort auf Buchungsanfragen gesendet werden. Die zusätzlichen Informationen geben Sie im Eingabefeld **Zusätzliche Daten** ein.
Zusätzliche Daten	Zusatzangaben zur Antwort auf Buchungsanfragen.
Anhänge aus Buchungsanfragen entfernen	Gibt an, ob Anlagen aus Buchungsanfragen gelöscht werden.
Kommentare aus Buchungsanfragen entfernen	Gibt an, ob Nachrichtentext aus Buchungsanfragen gelöscht wird.
Betreff aus Buchungsanfragen entfernen	Gibt an, ob der Betreff einer Buchungsanfrage gelöscht wird.
Nur Terminanlagen beibehalten	Gibt an, ob Elemente, die nicht zum Kalender gehören, gelöscht werden.
Antwortdetails aktivieren	Gibt an, ob die Gründe für die Annahme oder Ablehnung einer Besprechung zur Antwort-E-Mail hinzugefügt werden sollen.

Eigenschaft	Beschreibung
Neue Terminanfragen mit Status "Mit Vorbehalt" markieren	Gibt an, ob neue Terminanfragen automatisch mit dem Status **Mit Vorbehalt** in den Kalender eingetragen werden.
Buchungsanfragen mit Status "Mit Vorbehalt" markieren	Gibt an, ob Buchungsanfragen im Kalender mit dem Status **Mit Vorbehalt** gekennzeichnet werden. Ist die Option deaktiviert, werden Buchungsanfragen mit dem Status **Frei** gekennzeichnet.
Status "Privat" von Buchungsanfragen entfernen	Gibt an, ob der Status **Privat** für Buchungsanfragen gelöscht wird.
Terminweiterleitungen löschen	Gibt an, ob Benachrichtigungen über Weiterleitungen der Termine an weitere Teilnehmer automatisch gelöscht werden. Diese Benachrichtigungen werden in den Ordner **Gelöschte Elemente** verschoben.
Abgelaufene Terminanfragen löschen	Gibt an, ob veraltete Terminanfragen automatisch aus dem Kalender gelöscht werden.

Verwandte Themen

- Buchungsberechtigungen für Exchange Online Gerätepostfächer und Exchange Online Raumpostfächer konfigurieren auf Seite 112

Buchungsberechtigungen für Exchange Online Gerätepostfächer und Exchange Online Raumpostfächer konfigurieren

Für Gerätepostfächer und Raumpostfächer können Sie die Buchungsberechtigungen der Ressourcen konfigurieren.

Sofern die Buchung einer Ressource nicht zu einem Planungskonflikt führt oder Grenzwerte für die Ressource überschritten werden, wie beispielsweise die Raumkapazität oder die Planungsdauer, können Buchungsanfragen automatisch genehmigt werden.

Buchungsanfragen automatisch genehmigen, wenn die Ressource verfügbar ist

- Ist die Option **Buchungsberechtigung für alle** gesetzt, kann jeder Benutzer die Ressource mit einer Buchungsanfrage, die den Richtlinien entspricht, automatisch reservieren.

- Über die Aufgabe **Buchungsberechtigung zuweisen** sind einzelne Benutzer festgelegt, deren richtlinienkonforme Buchungsanfragen automatisch genehmigt werden.

Buchungsanfragen erlauben, wenn die Ressource verfügbar ist

- Ist die Option **Buchungsanfragenberechtigung für alle** gesetzt, dürfen alle Benutzer Buchungsanfragen, die den Richtlinien entsprechen, senden.
- Über die Aufgabe **Richtlinienkonforme Buchungsanfragen erlauben** sind einzelne Benutzer festgelegt, die Buchungsanfragen senden dürfen, die den Richtlinien entsprechen.

Buchungsanfragen automatisch genehmigen, wenn die Ressource verfügbar ist und Buchungsanfragen senden, wenn die Ressource nicht verfügbar ist

- Ist die Option **Richtlinienunabhängige Buchungsanfragenberechtigung für alle** gesetzt, kann jeder Benutzer die Ressource mit einer Buchungsanfrage, die den Richtlinien entspricht, automatisch reservieren. Die Benutzer dürfen Buchungsanfragen senden, die nicht den Richtlinien entsprechen. Buchungsanfragen, die nicht den Richtlinien genügen, können vom Stellvertreter des Postfachs genehmigt werden.
- Über die Aufgabe **Richtlinienunabhängige Buchungsanfragen erlauben** sind einzelne Benutzer festgelegt, deren richtlinienkonforme Buchungsanfragen automatisch genehmigt werden und die Buchungsanfragen senden dürfen, die nicht den Richtlinien entsprechen. Buchungsanfragen, die nicht den Richtlinien genügen, können vom Stellvertreter des Postfachs genehmigt werden.

Empfangsbeschränkungen für Exchange Online Postfächer anpassen

HINWEIS: Die Zuweisungen **Postannahme erlauben** und **Postannahme verweigern** schließen einander aus. Sie können entweder festlegen, ob die Nachrichten eines Empfängers akzeptiert werden oder abgelehnt werden.

Um die Postannahme für ein Postfach anzupassen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Postfächer**.
2. Wählen Sie in der Ergebnisliste das Postfach.
3. Wählen Sie die Aufgabe **Postannahme erlauben**, um festzulegen, von welchen Empfängern Nachrichten akzeptiert werden.

   - ODER -

Wählen Sie die Aufgabe **Postannahme verweigern**, um festzulegen, von welchen Empfängern Nachrichten abgelehnt werden.

4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Empfänger enthält. Zur Auswahl stehen:
    - E-Mail-aktivierte Verteilergruppen
    - Dynamische Verteilergruppen
    - Postfächer
    - E-Mail Benutzer
    - E-Mail Kontakte
    - Office 365 Gruppen
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Empfänger zu.

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

    Um eine Zuweisung zu entfernen

    - Wählen Sie den Empfänger und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Exchange Online Postfachberechtigung: Senden im Auftrag

Über die Sendeberechtigung **Senden im Auftrag von** legen Sie fest, welche Benutzer Benachrichtigungen im Auftrag des Postfachbesitzers senden können.

Um die Sendeberechtigung für ein Postfach anzupassen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Postfächer**.
2. Wählen Sie in der Ergebnisliste das Postfach.
3. Wählen Sie die Aufgabe **Sendeberechtigung zuweisen.**
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Benutzer enthält. Zur Auswahl stehen:
    - E-Mail-aktivierte Verteilergruppen
    - Postfächer
    - E-Mail Benutzer
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzer zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie den Benutzer und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online Postfachberechtigung: Senden als auf Seite 115
- Exchange Online Postfachberechtigung: Vollzugriff auf Seite 116

Exchange Online Postfachberechtigung: Senden als

Über die Postfachberechtigung **Senden als** legen Sie fest, welche Benutzer Benachrichtigungen über ein Postfach senden können. Die Benachrichtigung wird so angezeigt, als käme sie vom Postfachbesitzer.

Um die Postfachberechtigung für Postfächer anzupassen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Postfächer**.
2. Wählen Sie in der Ergebnisliste das Postfach.
3. Wählen Sie die Aufgabe **Senden als Berechtigungen zuweisen.**
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Benutzer enthält. Zur Auswahl stehen:
   - Azure Active Directory Benutzerkonten
   - Azure Active Directory Gruppen
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online Postfachberechtigung: Vollzugriff auf Seite 116
- Exchange Online Postfachberechtigung: Senden im Auftrag auf Seite 114

Exchange Online Postfachberechtigung: Vollzugriff

Mit der Postfachberechtigung **Vollzugriff** kann sich ein Benutzer an einem Postfach anmelden und den Inhalt des Postfach anzuzeigen und zu bearbeiten. Die Postfachberechtigung zum Senden von Benachrichtigungen aus diesem Postfach muss separat erteilt werden.

Um die Postfachberechtigung für Postfächer anzupassen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Postfächer**.
2. Wählen Sie in der Ergebnisliste das Postfach.
3. Wählen Sie die Aufgabe **Vollzugriff Berechtigungen zuweisen.**
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Benutzer enthält. Zur Auswahl stehen:
    - Azure Active Directory Benutzerkonten
    - Azure Active Directory Gruppen
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzer zu.

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

    Um eine Zuweisung zu entfernen

    - Wählen Sie den Benutzer und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online Postfachberechtigung: Senden im Auftrag auf Seite 114
- Exchange Online Postfachberechtigung: Senden als auf Seite 115

Moderatoren für Exchange Online Postfächer festlegen

Moderierte Postfächer werden eingesetzt, um Nachrichten an ein Postfach durch einen Moderator zu genehmigen oder abzulehnen. Erst nach Genehmigung durch den Moderator wird die Nachricht an das Postfach weitergeleitet.

Um Moderatoren für das Postfach festzulegen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Postfächer**.
2. Wählen Sie in der Ergebnisliste das Postfach.
3. Wählen Sie die Aufgabe **Moderatoren zuweisen**.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Benutzer enthält. Zur Auswahl stehen:
    - Postfächer
    - E-Mail Kontakte
    - E-Mail Benutzer
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Moderatoren zu.

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

    Um eine Zuweisung zu entfernen

    - Wählen Sie den Moderator und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Zusatzeigenschaften an Exchange Online Postfächer zuweisen

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

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

Um Zusatzeigenschaften für ein Postfach festzulegen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Postfächer**
2. Wählen Sie in der Ergebnisliste das Postfach.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

    Um eine Zuweisung zu entfernen

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

Exchange Online Postfächer löschen

Benutzerpostfächer werden gelöscht, indem den Benutzerkonten im Azure Active Directory die Abonnements entzogen werden.

Gerätepostfächer, Raumpostfächer und freigegebene Postfächer können Sie im One Identity Manager löschen. Beim Löschen eines Gerätepostfachs, Raumpostfachs oder und freigegebenen Postfachs wird zusätzlich das Azure Active Directory Benutzerkonto, das mit dem Postfach verknüpft ist, gelöscht.

Um ein Postfach zu löschen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Postfächer**.
2. Wählen Sie in der Ergebnisliste das Postfach.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Exchange Online E-Mail Benutzer

E-Mail Benutzer enthalten Informationen über Benutzer außerhalb der Exchange Online Organisation. E-Mail Benutzer erhalten eine mindestens eine E-Mail-Adresse. Benachrichtigungen werden automatisch an diese E-Mail-Adresse weitergeleitet. Im Gegensatz zu E-Mail Kontakten haben E-Mail Benutzer Anmeldeinformationen und können auf Ressourcen zugreifen.

E-Mail Benutzer werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können E-Mail Benutzer im One Identity Manager erstellen und bearbeiten. Beim Erzeugen eines E-Mail Benutzers wird zusätzlich ein Azure Active Directory Benutzerkonto erzeugt und mit dem E-Mail Benutzer verknüpft.

HINWEIS: Um E-Mail Benutzer für die Identitäten eines Unternehmens einzurichten, wird der Einsatz von Kontendefinitionen empfohlen.

- Um E-Mail Benutzer über Kontendefinitionen zu erzeugen, müssen die Identitäten ein zentrales Benutzerkonto und eine Standard-E-Mail-Adresse besitzen und über die Zuordnung zu einer primären Abteilung, einem primären Standort oder einer primären Kostenstelle ihre IT Betriebsdaten erhalten.
- Einige der Stammdaten der E-Mail Benutzer werden über Bildungsregeln aus den Identitätenstammdaten gebildet.

Detaillierte Informationen zum Thema

- Kontendefinitionen für Exchange Online E-Mail Benutzer und Exchange Online E-Mail Kontakte auf Seite 64
- Exchange Online E-Mail Benutzer erstellen auf Seite 120
- Stammdaten für Exchange Online E-Mail Benutzer bearbeiten auf Seite 121
- Stammdaten für Exchange Online E-Mail Benutzer auf Seite 121
- Empfangsbeschränkungen für Exchange Online E-Mail Benutzer anpassen auf Seite 127
- Sendeberechtigung für Exchange Online E-Mail Benutzer anpassen auf Seite 128
- Moderatoren für Exchange Online E-Mail Benutzer festlegen auf Seite 129
- Zusatzeigenschaften an Exchange Online E-Mail Benutzer zuweisen auf Seite 130

- Exchange Online E-Mail Benutzer löschen auf Seite 130
- Einzelobjekte synchronisieren auf Seite 53

Exchange Online E-Mail Benutzer erstellen

Beim Erzeugen eines E-Mail Benutzers wird zusätzlich ein Azure Active Directory Benutzerkonto erzeugt und mit dem E-Mail Benutzer verknüpft.

Für die Generierung von Zufallskennwörtern für neue E-Mail Benutzer, das Versenden der Anmeldeinformationen sowie die Verwendung von Kennwortrichtlinien werden die Konfigurationseinstellungen für Azure Active Directory genutzt. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung.*

HINWEIS: Um E-Mail Benutzer für die Identitäten eines Unternehmens einzurichten, wird der Einsatz von Kontendefinitionen empfohlen.

- Um E-Mail Benutzer über Kontendefinitionen zu erzeugen, müssen die Identitäten ein zentrales Benutzerkonto und eine Standard-E-Mail-Adresse besitzen und über die Zuordnung zu einer primären Abteilung, einem primären Standort oder einer primären Kostenstelle ihre IT Betriebsdaten erhalten.
- Einige der Stammdaten der E-Mail Benutzer werden über Bildungsregeln aus den Identitätenstammdaten gebildet.

Um einen E-Mail Benutzer zu erstellen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Benutzer**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular erfassen Sie die Stammdaten des E-Mail Benutzers.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Kontendefinitionen für Exchange Online E-Mail Benutzer und Exchange Online E-Mail Kontakte auf Seite 64
- Stammdaten für Exchange Online E-Mail Benutzer bearbeiten auf Seite 121
- Stammdaten für Exchange Online E-Mail Benutzer auf Seite 121

Stammdaten für Exchange Online E-Mail Benutzer bearbeiten

Um einen E-Mail Benutzer zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Benutzer**.
2. Wählen Sie in der Ergebnisliste den E-Mail Benutzer und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten des E-Mail Benutzers.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online E-Mail Benutzer erstellen auf Seite 120
- Stammdaten für Exchange Online E-Mail Benutzer auf Seite 121

Stammdaten für Exchange Online E-Mail Benutzer

Tabelle 17: Stammdaten eines E-Mail Benutzers

Eigenschaft	Beschreibung
Identität	Identität, die den E-Mail Benutzer verwendet. • Wurde der E-Mail Benutzer über eine Kontendefinition erzeugt, ist die Identität bereits eingetragen. • Wenn Sie den E-Mail Benutzer manuell erstellen, können Sie die Identität aus der Auswahlliste wählen. In der Auswahlliste werden im Standard aktivierte und deaktivierte Identitäten angezeigt. Um deaktivierte Identitäten nicht in der Auswahlliste anzuzeigen, aktivieren Sie den Konfigurationsparameter **QER | Person| HideDeactivatedIdentities**. HINWEIS: Wenn Sie eine deaktivierte Identität an einen E-Mail Benutzer zuordnen, wird der E-Mail Benutzer, abhängig von der Konfiguration, unter Umständen gesperrt oder gelöscht.
Keine Verbindung mit einer Identität erfor-	Gibt an, ob dem E-Mail Benutzer absichtlich keine Identität zugeordnet ist. Der Wert wird aus dem verbundenen

Eigenschaft	Beschreibung
derlich	Benutzerkonto ermittelt.
Nicht mit einer Identität verbunden	Zeigt an, warum für den E-Mail Benutzer die Option **Keine Verbindung mit einer Identität erforderlich** aktiviert ist. Der Wert wird aus dem verbundenen Benutzerkonto ermittelt. Mögliche Werte sind: • **durch Administrator**: Die Option wurde manuell durch den Administrator aktiviert. • **durch Attestierung**: Das Benutzerkonto wurde attestiert. • **durch Ausschlusskriterium**: Das Benutzerkonto wird aufgrund eines Ausschlusskriteriums nicht mit einer Identität verbunden. Das Benutzerkonto ist beispielsweise in der Ausschlussliste für die automatische Identitätenzuordnung enthalten (Konfigurationsparameter **PersonExcludeList**).
Kontendefinition	Kontendefinition, über die der E-Mail Benutzer erstellt wurde. Die Kontendefinition wird benutzt, um die Stammdaten des E-Mail Benutzers automatisch zu befüllen und um einen Automatisierungsgrad für den E-Mail Benutzer festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Identität und trägt sie in die entsprechenden Eingabefelder des E-Mail Benutzers ein. HINWEIS: Die Kontendefinition darf nach dem Speichern des E-Mail Benutzers nicht geändert werden.
Automatisierungsgrad	Automatisierungsgrad, mit dem der E-Mail Benutzer erstellt wird. Wählen Sie einen Automatisierungsgrad aus der Auswahlliste. Den Automatisierungsgrad können Sie nur festlegen, wenn Sie auch eine Kontendefinition eingetragen haben. In der Auswahlliste werden alle Automatisierungsgrade der gewählten Kontendefinition angeboten.
Azure Active Directory Mandant	Bezeichnung des Azure Active Directory Mandanten.
Azure Active Directory Benutzerkonto	Azure Active Directory Benutzerkonto, welches den E-Mail Benutzer verwendet.
Vorname	Vorname des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Nachname	Nachname des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automa-

Eigenschaft	Beschreibung
	tisierungsgrad automatisch ausgefüllt.
Initialen	Initialen des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Bezeichnung	Bezeichnung des E-Mail Benutzers.
Anzeigename	Anzeigename, wie er im Adressbuch verwendet wird.
Alias	Eindeutiger Alias zur weiteren Identifizierung des E-Mail Benutzers.

Benutzer-ID	Benutzer-ID, mit der sich der E-Mail Benutzer anmeldet.
	Beispiel:
	`<alias>@<domain.com>`
	`<user>@yourorganisation.onmicrosoft.com`

Kennwort	Kennwort für die Anmeldung. Das zentrale Kennwort der zugeordneten Identität kann auf das Kennwort des E-Mail-Benutzers abgebildet werden. Ausführliche Informationen zum zentralen Kennwort einer Identität finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*. HINWEIS: Beim Prüfen eines Benutzerkennwortes werden die One Identity Manager Kennwortrichtlinien beachtet. Stellen Sie sicher, dass die Kennwortrichtlinie nicht gegen die Anforderungen des Zielsystems verstößt. Für die Generierung von Zufallskennwörtern für neue E-Mail Benutzer, das Versenden der Anmeldeinformationen sowie die Verwendung von Kennwortrichtlinien werden die Konfigurationseinstellungen für Azure Active Directory genutzt. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung.*
Bestätigung	Kennwortwiederholung.
Proxy Adressen	Weitere E-Mail-Adressen zum E-Mail Benutzer. Für die Erstellung weiterer Proxy Adressen ist die folgende Syntax einzuhalten: `Adresstyp: neue E-Mail-Adresse`
Empfängertyp (Detail)	Typ des E-Mail-Benutzers. Zur Auswahl stehen **E-Mail-Benutzer** und **Gast-E-Mail-Benutzer**.
Externe E-Mail Adresse	E-Mail-Adresse, an welche die Nachrichten weitergeleitet werden sollen.

Eigenschaft	Beschreibung
Zieladresstyp	Adresstyp der E-Mail-Adresse. Zulässiger Wert ist **SMTP**.
Nicht in Adresslisten anzeigen	Gibt an, ob der E-Mail Benutzer in Adressbüchern angezeigt werden soll. Setzen Sie die Option, wenn Sie verhindern wollen, dass der E-Mail Benutzer in Adressbüchern angezeigt wird. Diese Option gilt für die Anzeige in allen Adressbüchern.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten Gruppen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen an den E-Mail Benutzer. Gruppen können selektiv an die E-Mail Benutzer vererbt werden. Dazu werden die Gruppen und die E-Mail Benutzer in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Gruppen erbbar	Gibt an, ob der E-Mail Benutzer Gruppen über die Identität erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an den E-Mail Benutzer vererbt. • Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt der E-Mail Benutzer diese Gruppen. • Wenn eine Identität eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt der E-Mail Benutzer diese Gruppe nur, wenn die Option aktiviert ist.
Einfache Anzeige	Einfacher Anzeigename für Systeme, die nicht alle Zeichen des normalen Anzeigenamens interpretieren können.
Phonetischer Anzeigename	Anzeigename in phonetischer Schreibweise. Wird verwendet, wenn die Aussprache und Schreibweise des Namens nicht übereinstimmen. Der phonetische Anzeigename wird beispielsweise verwendet, um die Empfänger im hierarchischen Adressbuch zu sortieren, wenn keine Reihenfolge angegeben ist. Die Sortierung erfolgt aufsteigend von A bis Z. Ist kein phonetischer Anzeigenamen eingetragen, erfolgt die Sortierung nach dem Anzeigenamen.
Reihenfolge	Gibt an, in welcher Reihenfolge die Empfänger im hierarchischen Adressbuch angezeigt werden. Je größer der

Eigenschaft	Beschreibung
	Wert desto höher die Rangfolge in der Sortierung. Ist keine Reihenfolge angegeben oder haben mehrere Einträge die gleiche Reihenfolge, erfolgt die Sortierung nach dem phonetischen Anzeigenamen.
Nachrichtenformat	Nachrichtenformat für Nachrichten, die an einen E-Mail Benutzer gesendet werden. Zulässige Werte sind **MIME** (Standard) und **Text**.
Format Nachrichtentext	Format des Nachrichtentextes für die Nachrichten, die an einen E-Mail Benutzer gesendet werden. Zur Auswahl stehen**Text**, **HTML** und **TextAndHtml**. Die zulässigen Werte sind abhängig vom gewählten Nachrichtenformat. • Wenn das Nachrichtenformat **MIME** festgelegt ist, kann das Format des Nachrichtentextes **Text**, **HTML** oder **TextAndHtml** (Standard) sein. • Wenn das Nachrichtenfromat **Text** festgelegt ist, kann das Format des Nachrichtentextes **Text** sein.
Anlagenformat	Anlagenformat des Apple Macintosh-Betriebssystems für Nachrichten, die an einen E-Mail Benutzer gesendet werden. Zur Auswahl stehen **BinHex** (Standard), **UuEncode**, **AppleSingle** und **AppleDouble**.
Bevorzugtes Nachrich-tenformat	Gibt an, ob die für den Empfänger konfigurierten Einstellungen für das Nachrichtenformat die globalen Einstellungen überschreiben sollen.
MAPI-RTF benutzen	Gibt an, ob der E-Mail Benutzer Nachrichten im MAPI-Format erhalten darf. Zur Auswahl stehen **Niemals**, **Immer** und **Nutze Standardeinstellungen**.
Absender-Authen-tifizierung anfordern	Gibt an, ob die Authentifizierungsinformationen von Absendern angefordert werden. Setzen Sie die Option, um zu verhindern, dass anonyme Absender Benachrichtigungen an den E-Mail Benutzer senden können.
Moderation aktiviert	Gibt an, ob der E-Mail Benutzer moderiert wird. Legen Sie die Moderatoren über die Aufgabe **Moderatoren zuweisen** fest. Anschließend aktivieren Sie die Option.
Senden der Benach-richtigung	Angabe, wie Absender benachrichtigt werden, wenn Sie ein Nachricht an einen moderierten E-Mail Benutzer senden. Zulässige Werte sind: • **Keine Benachrichtigung**: Es erfolgt keine Benachrichtigung der Absender.

Eigenschaft	Beschreibung
	• **Nur Absender der eigenen Organisation benachrichtigen**: Nur interne Absender erhalten eine Benachrichtigung. • **Alle Absender benachrichtigen**: Interne und externe Absender erhalten eine Benachrichtigung.
Straße	Straße. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Ort	Ort. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. Anhand des Ortes können automatisch Standorte erzeugt und den Identitäten zugeordnet werden.
Postfach	Postfach. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Bundesland	Bundesland. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Postleitzahl	Postleitzahl. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Land/Region	Länderkennung.
Büro	Büroanschrift.
Telefon (Geschäftlich)	Geschäftliche Telefonnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Weitere Telefon-nummern	Weitere geschäftliche Telefonnummern.
Fax	Faxnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Weitere Faxnummern	Weitere Faxnummern.
Telefon (Privat)	Private Telefonnummer.
Weitere Privatnummern	Weitere private Telefonnummern.
Mobiltelefon	Mobiltelefonnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.

Eigenschaft	Beschreibung
Funknummer	Funknummer.
Webseite	Webseite des Benutzers.
Notizen	Weitere Informationen zum Benutzer.
Position	Dienstbezeichnung des Benutzers.
Abteilung	Abteilung. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Firma	Firma. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Manager	Verantwortlicher für den E-Mail Benutzer. ***Um einen Manager festzulegen*** 1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. 2. Wählen Sie unter **Tabelle** die Tabelle, welche die Kontomanager abbildet. 3. Wählen Sie unter **Kontomanager** den Verantwortlichen. 4. Klicken Sie **OK**.
Assistent	Name des Assistenten des E-Mail Benutzers.

Verwandte Themen

- Kontendefinitionen für Exchange Online E-Mail Benutzer und Exchange Online E-Mail Kontakte auf Seite 64
- Moderatoren für Exchange Online Postfächer festlegen auf Seite 116
- Zuweisen von Exchange Online E-Mail-aktivierten Verteilergruppen an Exchange Online Empfänger auf Seite 153

Empfangsbeschränkungen für Exchange Online E-Mail Benutzer anpassen

HINWEIS: Die Zuweisungen **Postannahme erlauben** und **Postannahme verweigern** schließen einander aus. Sie können entweder festlegen, ob die Nachrichten eines Empfängers akzeptiert werden oder abgelehnt werden.

Um die Postannahme für einen E-Mail Benutzer anzupassen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Benutzer**.
2. Wählen Sie in der Ergebnisliste den E-Mail Benutzer.
3. Wählen Sie die Aufgabe **Postannahme erlauben**, um festzulegen, von welchen Empfängern Nachrichten akzeptiert werden.

   - ODER -

   Wählen Sie die Aufgabe **Postannahme verweigern**, um festzulegen, von welchen Empfängern Nachrichten abgelehnt werden.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Empfänger enthält. Zur Auswahl stehen:
   - E-Mail-aktivierte Verteilergruppen
   - Dynamische Verteilergruppen
   - Postfächer
   - E-Mail Benutzer
   - E-Mail Kontakte
   - Office 365 Gruppen
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Empfänger zu.

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

   Um eine Zuweisung zu entfernen
   - Wählen Sie den Empfänger und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Sendeberechtigung für Exchange Online E-Mail Benutzer anpassen

Über die Sendeberechtigung **Senden im Auftrag von** legen Sie fest, welche Benutzer Benachrichtigungen im Auftrag des E-Mail Benutzers senden können.

Um die Sendeberechtigung für einen E-Mail Benutzer anzupassen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Benutzer**.
2. Wählen Sie in der Ergebnisliste den E-Mail Benutzer.
3. Wählen Sie die Aufgabe **Sendeberechtigung zuweisen.**
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Benutzer enthält. Zur Auswahl stehen:

- E-Mail-aktivierte Verteilergruppen
- Postfächer
- E-Mail Benutzer

5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzer zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Benutzer und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Moderatoren für Exchange Online E-Mail Benutzer festlegen

Moderierte E-Mail Benutzer werden eingesetzt, um Nachrichten an einen E-Mail Benutzer durch einen Moderator zu genehmigen oder abzulehnen. Erst nach Genehmigung durch den Moderator wird die Nachricht an den E-Mail Benutzer weitergeleitet.

Um Moderatoren für einen E-Mail Benutzer festzulegen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Benutzer**.
2. Wählen Sie in der Ergebnisliste den E-Mail Benutzer.
3. Wählen Sie die Aufgabe **Moderatoren zuweisen**.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Benutzer enthält. Zur Auswahl stehen:
   - Postfächer
   - E-Mail Kontakte
   - E-Mail Benutzer
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Moderatoren zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Moderator und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Zusatzeigenschaften an Exchange Online E-Mail Benutzer zuweisen

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

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

Um Zusatzeigenschaften für einen E-Mail Benutzer festzulegen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Benutzer**.
2. Wählen Sie in der Ergebnisliste den E-Mail Benutzer.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

Exchange Online E-Mail Benutzer löschen

Beim Löschen eines E-Mail Benutzers wird die Option **Nicht in Adresslisten anzeigen** aktiviert und somit der E-Mail Benutzer nicht mehr in den Adressbüchern angezeigt. Beim Löschen eines E-Mail Benutzers wird zusätzlich das Azure Active Directory Benutzerkonto, das mit dem E-Mail Benutzer verknüpft ist, gelöscht.

HINWEIS: Solange eine Kontendefinition für eine Identität wirksam ist, behält die Identität ihren daraus entstandenen E-Mail Benutzer. Wird die Zuweisung einer Kontendefinition entfernt, dann wird der E-Mail Benutzer, der aus dieser Kontendefinition entstanden ist, gelöscht.

Um einen E-Mail Benutzer zu löschen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Benutzer**.
2. Wählen Sie in der Ergebnisliste den E-Mail Benutzer.

3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Exchange Online E-Mail Kontakte

E-Mail Kontakte enthalten Informationen über Benutzer außerhalb der Exchange Online Organisation. E-Mail Kontakte erhalten eine mindestens eine E-Mail-Adresse. Benachrichtigungen werden automatisch an diese E-Mail-Adresse weitergeleitet. Im Gegensatz zu E-Mail Benutzern haben E-Mail Kontakte keine Anmeldeinformationen und keinen Zugriff auf Ressourcen.

E-Mail Kontakte werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können E-Mail Kontakte im One Identity Manager erstellen und bearbeiten.

HINWEIS: Um E-Mail Kontakte für die Identitäten eines Unternehmens einzurichten, wird der Einsatz von Kontendefinitionen empfohlen.

- Um E-Mail Kontakte über Kontendefinitionen zu erzeugen, müssen die Identitäten ein zentrales Benutzerkonto und eine Standard-E-Mail-Adresse besitzen und über die Zuordnung zu einer primären Abteilung, einem primären Standort oder einer primären Kostenstelle ihre IT Betriebsdaten erhalten.
- Einige der Stammdaten der E-Mail Kontakte werden über Bildungsregeln aus den Identitätenstammdaten gebildet.

Detaillierte Informationen zum Thema

- Kontendefinitionen für Exchange Online E-Mail Benutzer und Exchange Online E-Mail Kontakte auf Seite 64
- Exchange Online E-Mail Kontakte erstellen auf Seite 133
- Stammdaten für Exchange Online E-Mail Kontakte bearbeiten auf Seite 133
- Stammdaten für Exchange Online E-Mail Kontakte auf Seite 134
- Empfangsbeschränkungen für Exchange Online E-Mail Kontakte anpassen auf Seite 140
- Sendeberechtigung für Exchange Online E-Mail Kontakte anpassen auf Seite 141
- Moderatoren für Exchange Online E-Mail Kontakte festlegen auf Seite 141
- Zusatzeigenschaften an Exchange Online E-Mail Kontakte zuweisen auf Seite 142
- Exchange Online E-Mail Kontakte löschen auf Seite 143
- Einzelobjekte synchronisieren auf Seite 53

Exchange Online E-Mail Kontakte erstellen

HINWEIS: Um E-Mail Kontakte für die Identitäten eines Unternehmens einzurichten, wird der Einsatz von Kontendefinitionen empfohlen.

- Um E-Mail Kontakte über Kontendefinitionen zu erzeugen, müssen die Identitäten ein zentrales Benutzerkonto und eine Standard-E-Mail-Adresse besitzen und über die Zuordnung zu einer primären Abteilung, einem primären Standort oder einer primären Kostenstelle ihre IT Betriebsdaten erhalten.
- Einige der Stammdaten der E-Mail Kontakte werden über Bildungsregeln aus den Identitätenstammdaten gebildet.

Um einen E-Mail Kontakt zu erstellen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Kontakte**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular erfassen Sie die Stammdaten des E-Mail Kontaktes.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Kontendefinitionen für Exchange Online E-Mail Benutzer und Exchange Online E-Mail Kontakte auf Seite 64
- Stammdaten für Exchange Online E-Mail Kontakte bearbeiten auf Seite 133
- Stammdaten für Exchange Online E-Mail Kontakte auf Seite 134

Stammdaten für Exchange Online E-Mail Kontakte bearbeiten

Um einen E-Mail Kontakt zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Kontakte**.
2. Wählen Sie in der Ergebnisliste den E-Mail Kontakt und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten des E-Mail Kontaktes.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online E-Mail Kontakte erstellen auf Seite 133
- Stammdaten für Exchange Online E-Mail Kontakte auf Seite 134

Stammdaten für Exchange Online E-Mail Kontakte

Tabelle 18: Stammdaten eines E-Mail Kontaktes

Eigenschaft	Beschreibung
Identität	Identität, die den E-Mail Kontakt verwendet. • Wurde der E-Mail Kontakt über eine Kontendefinition erzeugt, ist die Identität bereits eingetragen. • Wenn Sie den E-Mail Kontakt manuell erstellen, können Sie die Identität aus der Auswahlliste wählen. In der Auswahlliste werden im Standard aktivierte und deaktivierte Identitäten angezeigt. Um deaktivierte Identitäten nicht in der Auswahlliste anzuzeigen, aktivieren Sie den Konfigurationsparameter **QER | Person| HideDeactivatedIdentities**. HINWEIS: Wenn Sie eine deaktivierte Identität an einen E-Mail Kontakt zuordnen, wird der E-Mail Kontakt, abhängig von der Konfiguration, unter Umständen gesperrt oder gelöscht.
Keine Verbindung mit einer Identität erforderlich	Gibt an, ob dem Kontakt absichtlich keine Identität zugeordnet ist. Die Option wird automatisch aktiviert, wenn ein Kontakt in der Ausschlussliste für die automatische Identitätenzuordnung enthalten ist oder eine entsprechende Attestierung erfolgt ist. Sie können die Option manuell setzen. Aktivieren Sie die Option, falls der Kontakt mit keiner Identität verbunden werden muss (beispielsweise, wenn mehrere Identitäten den Kontakt verwenden). Wenn durch die Attestierung diese Kontakte genehmigt werden, werden diese Kontakte künftig nicht mehr zur Attestierung vorgelegt. Im Web Portal können Kontakte, die nicht mit einer Identität verbunden sind, nach verschiedenen Kriterien gefiltert werden.
Nicht mit einer Identität verbunden	Zeigt an, warum für den Kontakt die Option **Keine Verbindung mit einer Identität erforderlich** aktiviert ist. Mögliche Werte sind:

Eigenschaft	Beschreibung
	• **durch Administrator**: Die Option wurde manuell durch den Administrator aktiviert. • **durch Attestierung**: Der Kontakt wurde attestiert. • **durch Ausschlusskriterium**: Der Kontakt wird aufgrund eines Ausschlusskriteriums nicht mit einer Identität verbunden. Der Kontakt ist beispielsweise in der Ausschlussliste für die automatische Identitätenzuordnung enthalten (Konfigurationsparameter **PersonExcludeList**).
Kontendefinition	Kontendefinition, über die der E-Mail Kontakt erstellt wurde. Die Kontendefinition wird benutzt, um die Stammdaten des E-Mail Kontaktes automatisch zu befüllen und um einen Automatisierungsgrad für den E-Mail Kontakt festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Identität und trägt sie in die entsprechenden Eingabefelder des E-Mail Kontaktes ein. HINWEIS: Die Kontendefinition darf nach dem Speichern des E-Mail Kontaktes nicht geändert werden.
Automatisierungsgrad	Automatisierungsgrad, mit dem der E-Mail Kontakt erstellt wird. Wählen Sie einen Automatisierungsgrad aus der Auswahlliste. Den Automatisierungsgrad können Sie nur festlegen, wenn Sie auch eine Kontendefinition eingetragen haben. In der Auswahlliste werden alle Automatisierungsgrade der gewählten Kontendefinition angeboten.
Azure Active Directory Mandant	Bezeichnung des Azure Active Directory Mandanten.
Vorname	Vorname des Kontaktes. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Nachname	Nachname des Kontaktes. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Initialen	Initialen des Kontaktes. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Bezeichnung	Bezeichnung des E-Mail Kontaktes.
Anzeigename	Anzeigename, wie er im Adressbuch verwendet wird.
Alias	Eindeutiger Alias zur weiteren Identifizierung des E-Mail Kontaktes.

Eigenschaft	Beschreibung
Proxy Adressen	Weitere E-Mail-Adressen zum E-Mail Kontakt. Für die Erstellung weiterer Proxy Adressen ist die folgende Syntax einzuhalten: `Adresstyp: neue E-Mail-Adresse`
Externe E-Mail Adresse	E-Mail-Adresse, an welche die Nachrichten weitergeleitet werden sollen.
Zieladresstyp	Adresstyp der E-Mail-Adresse. Zulässiger Wert ist **SMTP**.
Nicht in Adresslisten anzeigen	Gibt an, ob der E-Mail Kontakt in Adressbüchern angezeigt werden soll. Setzen Sie die Option, wenn Sie verhindern wollen, dass der E-Mail Kontakt in Adressbüchern angezeigt wird. Diese Option gilt für die Anzeige in allen Adressbüchern.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten Gruppen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen an den E-Mail Kontakt. Gruppen können selektiv an die E-Mail Kontakte vererbt werden. Dazu werden die Gruppen und die E-Mail Kontakte in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Gruppen erbbar	Gibt an, ob der E-Mail Kontakt Gruppen über die Identität erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an den E-Mail Kontakt vererbt. • Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt der E-Mail Kontakt diese Gruppen. • Wenn eine Identität eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt der E-Mail Kontakt diese Gruppe nur, wenn die Option aktiviert ist.
Einfache Anzeige	Einfacher Anzeigename für Systeme, die nicht alle Zeichen des normalen Anzeigenamens interpretieren können.
Phonetischer Anzeigename	Anzeigename in phonetischer Schreibweise. Wird verwendet, wenn die Aussprache und Schreibweise des Namens nicht übereinstimmen. Der phonetische Anzeigename wird beispielsweise verwendet, um die Empfänger im hierarchischen Adressbuch zu sortieren, wenn keine Reihenfolge angegeben

Eigenschaft	Beschreibung
	ist. Die Sortierung erfolgt aufsteigend von A bis Z. Ist kein phonetischer Anzeigenamen eingetragen, erfolgt die Sortierung nach dem Anzeigenamen.
Reihenfolge	Gibt an, in welcher Reihenfolge die Empfänger im hierarchischen Adressbuch angezeigt werden. Je größer der Wert desto höher die Rangfolge in der Sortierung. Ist keine Reihenfolge angegeben oder haben mehrere Einträge die gleiche Reihenfolge, erfolgt die Sortierung nach dem phonetischen Anzeigenamen.
Nachrichtenformat	Nachrichtenformat für Nachrichten, die an einen E-Mail Kontakt gesendet werden. Zulässige Werte sind **MIME** (Standard) und **Text**.
Format Nachrichtentext	Format des Nachrichtentextes für die Nachrichten, die an einen E-Mail Kontakt gesendet werden. Zur Auswahl stehen**Text**, **HTML** und **TextAndHtml**. Die zulässigen Werte sind abhängig vom gewählten Nachrichtenformat. • Wenn das Nachrichtenformat **MIME** festgelegt ist, kann das Format des Nachrichtentextes **Text**, **HTML** oder **TextAndHtml** (Standard) sein. • Wenn das Nachrichtenfromat **Text** festgelegt ist, kann das Format des Nachrichtentextes **Text** sein.
Anlagenformat	Anlagenformat des Apple Macintosh-Betriebssystems für Nachrichten, die an einen E-Mail Kontakt gesendet werden. Zur Auswahl stehen **BinHex** (Standard), **UuEncode**, **AppleSingle** und **AppleDouble**.
Bevorzugtes Nachrich-tenformat	Gibt an, ob die für den Empfänger konfigurierten Einstellungen für das Nachrichtenformat die globalen Einstellungen überschreiben sollen.
MAPI-RTF benutzen	Gibt an, ob der E-Mail Kontakt Nachrichten im MAPI-Format erhalten darf. Zur Auswahl stehen **Niemals**, **Immer** und **Nutze Standardeinstellungen**.
Absender-Authen-tifizierung anfordern	Gibt an, ob die Authentifizierungsinformationen von Absendern angefordert werden. Setzen Sie die Option, um zu verhindern, dass anonyme Absender Benachrichtigungen an den E-Mail Kontakt senden können.
Moderation aktiviert	Gibt an, ob der E-Mail Kontakt moderiert wird. Legen Sie die Moderatoren über die Aufgabe **Moderatoren zuweisen** fest. Anschließend aktivieren Sie die Option.

Eigenschaft	Beschreibung
Senden der Benachrichtigung	Angabe, wie Absender benachrichtigt werden, wenn Sie ein Nachricht an einen moderierten E-Mail Kontakt senden. Zulässige Werte sind: • **Keine Benachrichtigung**: Es erfolgt keine Benachrichtigung der Absender. • **Nur Absender der eigenen Organisation benachrichtigen**: Nur interne Absender erhalten eine Benachrichtigung. • **Alle Absender benachrichtigen**: Interne und externe Absender erhalten eine Benachrichtigung.
Straße	Straße. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Ort	Ort. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. Anhand des Ortes können automatisch Standorte erzeugt und den Identitäten zugeordnet werden.
Postfach	Postfach. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Bundesland	Bundesland. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Postleitzahl	Postleitzahl. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Land/Region	Länderkennung.
Büro	Büroanschrift.
Telefon (Geschäftlich)	Geschäftliche Telefonnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Weitere Telefonnummern	Weitere geschäftliche Telefonnummern.
Fax	Faxnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Weitere Faxnummern	Weitere Faxnummern.

Eigenschaft	Beschreibung
Telefon (Privat)	Private Telefonnummer.
Weitere Privatnummern	Weitere private Telefonnummern.
Mobiltelefon	Mobiltelefonnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Funknummer	Funknummer.
Webseite	Webseite des Kontaktes.
Notizen	Weitere Informationen zum Kontakt.
Position	Dienstbezeichnung des Kontaktes.
Abteilung	Abteilung. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Firma	Firma. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Manager	Verantwortlicher für den E-Mail Kontakt. ***Um einen Manager festzulegen*** 1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. 2. Wählen Sie unter **Tabelle** die Tabelle, welche die Kontomanager abbildet. 3. Wählen Sie unter **Manager** den Verantwortlichen. 4. Klicken Sie **OK**.
Assistent	Name des Assistenten des E-Mail Kontaktes.
Telefon (Assistent)	Telefonnummer des Assistenten.

Verwandte Themen

- Kontendefinitionen für Exchange Online E-Mail Benutzer und Exchange Online E-Mail Kontakte auf Seite 64
- Moderatoren für Exchange Online E-Mail Kontakte festlegen auf Seite 141
- Zuweisen von Exchange Online E-Mail-aktivierten Verteilergruppen an Exchange Online Empfänger auf Seite 153

Empfangsbeschränkungen für Exchange Online E-Mail Kontakte anpassen

HINWEIS: Die Zuweisungen **Postannahme erlauben** und **Postannahme verweigern** schließen einander aus. Sie können entweder festlegen, ob die Nachrichten eines Empfängers akzeptiert werden oder abgelehnt werden.

Um die Postannahme für einen E-Mail Kontakt anzupassen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Kontakte**.
2. Wählen Sie in der Ergebnisliste den E-Mail Kontakt.
3. Wählen Sie die Aufgabe **Postannahme erlauben**, um festzulegen, von welchen Empfängern Nachrichten akzeptiert werden.

   - ODER -

   Wählen Sie die Aufgabe **Postannahme verweigern**, um festzulegen, von welchen Empfängern Nachrichten abgelehnt werden.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Empfänger enthält. Zur Auswahl stehen:
   - E-Mail-aktivierte Verteilergruppen
   - Dynamische Verteilergruppen
   - Postfächer
   - E-Mail Benutzer
   - E-Mail Kontakte
   - Office 365 Gruppen
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Empfänger zu.

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

   Um eine Zuweisung zu entfernen
   - Wählen Sie den Empfänger und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Sendeberechtigung für Exchange Online E-Mail Kontakte anpassen

Über die Sendeberechtigung **Senden im Auftrag von** legen Sie fest, welche Benutzer Benachrichtigungen im Auftrag des E-Mail Kontaktes senden können.

Um die Sendeberechtigung für einen E-Mail Kontakt anzupassen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Kontakte**.
2. Wählen Sie in der Ergebnisliste den E-Mail Kontakt.
3. Wählen Sie die Aufgabe **Sendeberechtigung zuweisen.**
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Benutzer enthält. Zur Auswahl stehen:
    - E-Mail-aktivierte Verteilergruppen
    - Postfächer
    - E-Mail Benutzer
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzer zu.

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

    Um eine Zuweisung zu entfernen

    - Wählen Sie den Benutzer und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Moderatoren für Exchange Online E-Mail Kontakte festlegen

Moderierte E-Mail Kontakte werden eingesetzt, um Nachrichten an einen E-Mail Kontakt durch einen Moderator zu genehmigen oder abzulehnen. Erst nach Genehmigung durch den Moderator wird die Nachricht an den E-Mail Kontakt weitergeleitet.

Um Moderatoren für einen E-Mail Kontakt festzulegen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Kontakte**.
2. Wählen Sie in der Ergebnisliste den E-Mail Kontakt.
3. Wählen Sie die Aufgabe **Moderatoren zuweisen**.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Benutzer enthält. Zur Auswahl stehen:

- Postfächer
- E-Mail Kontakte
- E-Mail Benutzer

5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Moderatoren zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Moderator und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Zusatzeigenschaften an Exchange Online E-Mail Kontakte zuweisen

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

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

Um Zusatzeigenschaften für einen E-Mail Kontakt festzulegen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Kontakte**.
2. Wählen Sie in der Ergebnisliste den E-Mail Kontakt.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Zusatzeigenschaft und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Exchange Online E-Mail Kontakte löschen

HINWEIS: Solange eine Kontendefinition für eine Identität wirksam ist, behält die Identität ihren daraus entstandenen E-Mail Kontakt. Wird die Zuweisung einer Kontendefinition entfernt, dann wird der E-Mail Kontakt, der aus dieser Kontendefinition entstanden ist, gelöscht.

Beim Löschen eines E-Mail Kontaktes wird die Option **Nicht in Adresslisten anzeigen** aktiviert und somit der E-Mail Kontakt nicht mehr in den Adressbüchern angezeigt.

Um einen E-Mail Kontakt zu löschen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Kontakte**.
2. Wählen Sie in der Ergebnisliste den E-Mail Kontakt.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Exchange Online E-Mail-aktivierte Verteilergruppen

Um Nachrichten an eine Gruppe von Empfängern zu verteilen, können E-Mail-aktivierte universelle Verteilergruppen und E-Mail-aktivierte universelle Sicherheitsgruppen verwendet werden.

E-Mail-aktivierte Verteilergruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können E-Mail-aktivierte Verteilergruppen im One Identity Manager erstellen und bearbeiten. Beim Erzeugen einer E-Mail-aktivierten Verteilergruppe wird zusätzlich eine Azure Active Directory Gruppe erzeugt und mit der E-Mail-aktivierten Verteilergruppe verknüpft.

Im One Identity Manager können Sie die E-Mail-aktivierten Verteilergruppen direkt an die Postfächer, E-Mail Benutzer und E-Mail Kontakte zuweisen oder über Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen vererben. Des Weiteren können Benutzer die E-Mail-aktivierten Verteilergruppen über das Web Portal bestellen. Dazu werden die E-Mail-aktivierten Verteilergruppen im IT Shop bereitgestellt.

Detaillierte Informationen zum Thema

- Vererbung von Exchange Online E-Mail-aktivierten Verteilergruppen anhand von Kategorien auf Seite 167
- Exchange Online E-Mail-aktivierte Verteilergruppen in Exchange Online E-Mail-aktivierte Verteilergruppen aufnehmen auf Seite 168
- Exchange Online dynamische Verteilergruppen in Exchange Online E-Mail-aktivierte Verteilergruppen aufnehmen auf Seite 168
- Exchange Online E-Mail-aktivierte öffentliche Ordner an Exchange Online E-Mail-aktivierte Verteilergruppen zuweisen auf Seite 169
- Zusatzeigenschaften an Exchange Online E-Mail-aktivierte Verteilergruppen zuweisen auf Seite 170
- Exchange Online E-Mail-aktivierte Verteilergruppen löschen auf Seite 170
- Einzelobjekte synchronisieren auf Seite 53

Exchange Online E-Mail-aktivierte Verteilergruppen erstellen

Beim Erzeugen einer E-Mail-aktivierten Verteilergruppe wird zusätzlich eine Azure Active Directory Gruppe erzeugt und mit der E-Mail-aktivierten Verteilergruppe verknüpft.

Um eine E-Mail-aktivierte Verteilergruppe zu erstellen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular erfassen Sie die Stammdaten der E-Mail-aktivierten Verteilergruppe.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Exchange Online E-Mail-aktivierte Verteilergruppen bearbeiten auf Seite 146
- Stammdaten für Exchange Online E-Mail-aktivierte Verteilergruppen auf Seite 146

Stammdaten für Exchange Online E-Mail-aktivierte Verteilergruppen bearbeiten

Um eine E-Mail-aktivierte Verteilergruppe zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten der E-Mail-aktivierten Verteilergruppe.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online E-Mail-aktivierte Verteilergruppen erstellen auf Seite 145
- Stammdaten für Exchange Online E-Mail-aktivierte Verteilergruppen auf Seite 146

Stammdaten für Exchange Online E-Mail-aktivierte Verteilergruppen

Tabelle 19: Stammdaten einer E-Mail-aktivierten Verteilergruppe

Eigenschaft	Beschreibung
Azure Active Directory Gruppe	Azure Active Directory Gruppe, für welche eine E-Mail-aktivierte Verteilergruppe erzeugt wird.
Azure Active Directory Mandant	Bezeichnung des Azure Active Directory Mandanten.
Bezeichnung	Bezeichnung der E-Mail-aktivierten Verteilergruppe.
Einfache Anzeige	Einfacher Anzeigename für Systeme, die nicht alle Zeichen des normalen Anzeigenamens interpretieren können.
Phonetischer Anzeigename	Anzeigename in phonetischer Schreibweise. Wird verwendet, wenn die Aussprache und Schreibweise des Namens nicht übereinstimmen. Der phonetische Anzeigename wird beispielsweise verwendet, um die Empfänger im hierarchischen Adressbuch zu sortieren, wenn keine Reihenfolge angegeben ist. Die Sortierung erfolgt aufsteigend von A bis Z.

Eigenschaft	Beschreibung
	Ist kein phonetischer Anzeigenamen eingetragen, erfolgt die Sortierung nach dem Anzeigenamen.
Reihenfolge	Gibt an, in welcher Reihenfolge die Empfänger im hierarchischen Adressbuch angezeigt werden. Je größer der Wert desto höher die Rangfolge in der Sortierung. Ist keine Reihenfolge angegeben oder haben mehrere Einträge die gleiche Reihenfolge, erfolgt die Sortierung nach dem phonetischen Anzeigenamen.
Anzeigename	Anzeigename, wie er im Adressbuch verwendet wird.
Alias	Eindeutiger Alias zur weiteren Identifizierung der E-Mail-aktivierten Verteilergruppe.
Gruppentyp	Typ der Gruppe. Zulässige Werte sind **Universell** (Standard) und **Universell, sicherheitsaktiviert**.
Proxy Adressen	E-Mail-Adressen zur E-Mail-aktivierten Verteilergruppe. Als Adresstyp können Sie zusätzlich zur Standardadressierung (SMTP, X400) weitere Mailkonnektoren (beispielsweise CCMail, MS) nutzen. Für die Erstellung weiterer Proxyadressen ist die folgende Syntax einzuhalten: `Adresstyp: neue E-Mail-Adresse`
Nicht in Adresslisten anzeigen	Gibt an, ob die E-Mail-aktivierte Verteilergruppe in Adressbüchern angezeigt werden soll. Setzen Sie die Option, wenn Sie verhindern wollen, dass die E-Mail-aktivierte Verteilergruppe in Adressbüchern angezeigt wird. Diese Option gilt für die Anzeige in allen Adressbüchern.
E-Mail Adresse	E-Mail Adresse der E-Mail-aktivierten Verteilergruppe.
Bericht an Absender	Gibt an, ob Zustellberichte an den Absender einer Nachricht gesendet werden sollen.
Bericht an Eigentümer	Gibt an, ob Zustellberichte an den Besitzer einer Nachricht gesendet werden sollen.
Nur Nachrichten authentifizierter Benutzer einschränken	Gibt an, ob die Authentifizierungsinformationen von Absendern angefordert werden. Setzen Sie die Option, wenn Nachrichten nur von authentifizierten Benutzern zulässig sind.
Abwesenheitsnotiz an Absender	Setzen Sie die Option, wenn die Absender von Nachrichten Abwesenheitsnachrichten erhalten sollen.
Aufnahme in die Gruppe	Angabe, wie Benutzer der E-Mail-aktivierte Verteilergruppe beitreten können. Zulässige Werte sind:

Eigenschaft	Beschreibung
	• **Offen**: Mitglieder können ohne Genehmigung in die Gruppe aufgenommen werden. • **Geschlossen**: Nur Administratoren der E-Mail-aktivierten Verteilergruppe können Mitglieder in die Gruppe aufnehmen. Anfragen zur Aufnahme in die Gruppe werden automatisch abgelehnt. • **Freigabe durch Eigner**: Anfragen zur Aufnahme in die Gruppe können gestellt werden und werden durch die Administratoren der Verteilergruppe genehmigt. Die Administratoren legen Sie über die Aufgabe **Administratoren zuweisen** fest.
Verlassen der Gruppe	Angabe, wie Benutzer die E-Mail-aktivierte Verteilergruppe verlassen können. Zulässige Werte sind: • **Offen**: Die Gruppe kann ohne Genehmigung verlassen werden. • **Geschlossen**: Die Gruppe kann nur mit Genehmigung des Administrators verlassen werden. Anfragen zum Verlassen der Gruppe werden automatisch abgelehnt. Die Administratoren legen Sie über die Aufgabe **Administratoren zuweisen** fest.
Moderation aktiviert	Gibt an, ob die E-Mail-aktivierte Verteilergruppe moderiert wird. Aktivieren Sie diese Option, wenn die Verteilergruppe moderiert werden soll. Die Moderatoren legen Sie über die Aufgabe **Moderatoren zuweisen** fest.
Moderation untergeordneter Gruppen erlaubt	Angabe, wie die Nachrichtengenehmigung zu verarbeiten ist, wenn eine moderierte Gruppe andere moderierte Gruppen als Mitglieder aufweist.
Senden der Benachrichtigung	Angabe, wie Absender benachrichtigt werden, wenn Sie ein Nachricht an eine moderierte Verteilergruppe senden. Zulässige Werte sind: • **Keine Benachrichtigung**: Es erfolgt keine Benachrichtigung der Absender. • **Nur Absender der eigenen Exchange Organisation benachrichtigen**: Nur interne Absender erhalten eine Benachrichtigung. • **Alle Absender benachrichtigen**: Interne und externe Absender erhalten eine Benachrichtigung.
IT Shop	Gibt an, ob die Gruppe über den IT Shop bestellbar ist. Ist die

Eigenschaft	Beschreibung
	Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Postfächer, E-Mail Benutzer und E-Mail Kontakte und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Postfächer, E-Mail Benutzer und E-Mail Kontakte ist nicht zulässig.
Leistungsposition	Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Postfächer, E-Mail Benutzer und E-Mail Kontakte. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen zur Risikobewertung finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen an Postfächer, E-Mail Benutzer und E-Mail Kontakte. Gruppen können selektiv an die Postfächer, E-Mail Benutzer und E-Mail Kontakte vererbt werden. Dazu werden die Gruppen und die Postfächer, E-Mail Benutzer und E-Mail Kontakte in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.

Verwandte Themen

- Moderatoren für Exchange Online E-Mail-aktivierte Verteilergruppen festlegen auf Seite 151
- Administratoren für Exchange Online E-Mail-aktivierte Verteilergruppen festlegen auf Seite 152

Empfangsbeschränkungen für Exchange Online E-Mail-aktivierte Verteilergruppen anpassen

HINWEIS: Die Zuweisungen **Postannahme erlauben** und **Postannahme verweigern** schließen einander aus. Sie können entweder festlegen, ob die Nachrichten eines Empfängers akzeptiert werden oder abgelehnt werden.

Um die Postannahme für E-Mail-aktivierte Verteilergruppen anzupassen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **Postannahme erlauben**, um festzulegen, von welchen Empfängern Nachrichten akzeptiert werden.

   - ODER -

   Wählen Sie die Aufgabe **Postannahme verweigern**, um festzulegen, von welchen Empfängern Nachrichten abgelehnt werden.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Empfänger enthält. Zur Auswahl stehen:
   - E-Mail-aktivierte Verteilergruppen
   - Dynamische Verteilergruppen
   - Postfächer
   - E-Mail Benutzer
   - E-Mail Kontakte
   - Office 365 Gruppen
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Empfänger zu.

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

   Um eine Zuweisung zu entfernen
   - Wählen Sie den Empfänger und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Sendeberechtigungen für Exchange Online E-Mail-aktivierte Verteilergruppen anpassen

Über die Sendeberechtigung **Senden im Auftrag von** legen Sie fest, welche Benutzer Benachrichtigungen im Auftrag der Verteilergruppe senden können.

Um die Sendeberechtigung für E-Mail-aktivierte Verteilergruppen anzupassen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **Sendeberechtigung zuweisen.**
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Benutzer enthält. Zur Auswahl stehen:
    - E-Mail-aktivierte Verteilergruppen
    - Postfächer
    - E-Mail Benutzer
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzer zu.

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

    Um eine Zuweisung zu entfernen

    - Wählen Sie den Benutzer und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Moderatoren für Exchange Online E-Mail-aktivierte Verteilergruppen festlegen

Moderierte Verteilergruppen werden eingesetzt, um Nachrichten an eine E-Mail-aktivierte Verteilergruppe durch einen Moderator zu genehmigen oder abzulehnen. Erst nach Genehmigung durch den Moderator wird die Nachricht an die Mitglieder der E-Mail-aktivierten Verteilergruppe weitergeleitet.

Um Moderatoren für eine E-Mail-aktivierte Verteilergruppe festzulegen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **Moderatoren zuweisen**.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Benutzer enthält. Zur Auswahl stehen:
    - Postfächer
    - E-Mail Kontakte
    - E-Mail Benutzer
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Moderatoren zu.

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

    Um eine Zuweisung zu entfernen

    - Wählen Sie den Moderator und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Administratoren für Exchange Online E-Mail-aktivierte Verteilergruppen festlegen

Mitgliedschaften in E-Mail-aktivierten Verteilergruppen können beantragt und genehmigt werden. Legen Sie fest, welche Benutzer die Verteilergruppe verwalten und somit über die Mitgliedschaften in der E-Mail-aktivierten Verteilergruppe entscheidungsberechtigt sind.

Um Administratoren einer E-Mail-aktivierten Verteilergruppe festzulegen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **Administratoren zuweisen**.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Administratoren enthält. Zur Auswahl stehen:
    - Azure Active Directory Benutzerkonten
    - E-Mail-aktivierte Verteilergruppen
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Administratoren zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie den Administrator und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Löschen Sie diesen Text und ersetzen Sie ihn mit Ihrem eigenen.

Zuweisen von Exchange Online E-Mail-aktivierten Verteilergruppen an Exchange Online Empfänger

Exchange Online E-Mail-aktivierte Verteilergruppen können indirekt oder direkt an Postfächer, E-Mail Benutzer und E-Mail Kontakte zugewiesen werden.

Bei der indirekten Zuweisung werden Identitäten und E-Mail-aktivierte Verteilergruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die E-Mail-aktivierten Verteilergruppen berechnet, die einer Identität zugewiesen sind.

- Wenn Sie eine Identität in Rollen aufnehmen und die Identität ein Postfach besitzt, dann wird dieses Postfach in die E-Mail-aktivierten Verteilergruppen aufgenommen.
- Wenn Sie eine Identität in Rollen aufnehmen und die Identität einen E-Mail Benutzer besitzt, dann wird dieser E-Mail Benutzer in die E-Mail-aktivierten Verteilergruppen aufgenommen.
- Wenn Sie eine Identität in Rollen aufnehmen und die Identität einen E-Mail Kontakt besitzt, dann wird dieser E-Mail Kontakt in die E-Mail-aktivierten Verteilergruppen aufgenommen.

Des Weiteren können Exchange Online E-Mail-aktivierte Verteilergruppen im Web Portal bestellt werden. Dazu werden Identitäten als Kunden in einen Shop aufgenommen. Alle Exchange Online E-Mail-aktivierten Verteilergruppen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Exchange Online E-Mail-aktivierte Verteilergruppen werden nach erfolgreicher Genehmigung den Identitäten zugewiesen.

Über Systemrollen können Exchange Online E-Mail-aktivierte Verteilergruppen zusammengefasst und als Paket an Identitäten und Arbeitsplätze zugewiesen werden. Sie können Systemrollen erstellen, die ausschließlich Exchange Online E-Mail-aktivierte Verteilergruppen enthalten. Ebenso können Sie in einer Systemrolle beliebige Unternehmensressourcen zusammenfassen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Exchange Online E-Mail-aktivierte Verteilergruppen auch direkt an Postfächer, E-Mail Benutzer und E-Mail Kontakte zuweisen.

Ausführliche Informationen finden Sie in den folgenden Handbüchern.

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

Detaillierte Informationen zum Thema

- Voraussetzungen für indirekte Zuweisungen von Exchange Online E-Mail-aktivierten Verteilergruppen auf Seite 154
- Exchange Online E-Mail-aktivierte Verteilergruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 156
- Exchange Online E-Mail-aktivierte Verteilergruppen an Geschäftsrollen zuweisen auf Seite 157
- Exchange Online E-Mail-aktivierte Verteilergruppen in Systemrollen aufnehmen auf Seite 159
- Exchange Online E-Mail-aktivierte Verteilergruppen in den IT Shop aufnehmen auf Seite 160
- Exchange Online Empfänger direkt an Exchange Online E-Mail-aktivierte Verteilergruppen zuweisen auf Seite 164
- Exchange Online E-Mail-aktivierte Verteilergruppen direkt an Exchange Online Postfächer zuweisen auf Seite 165
- Exchange Online E-Mail-aktivierte Verteilergruppen direkt an Exchange Online E-Mail Benutzer zuweisen auf Seite 165
- Exchange Online E-Mail-aktivierte Verteilergruppen direkt an Exchange Online E-Mail Kontakte zuweisen auf Seite 166

Voraussetzungen für indirekte Zuweisungen von Exchange Online E-Mail-aktivierten Verteilergruppen

Bei der indirekten Zuweisung werden Identitäten und Exchange OnlineE-Mail-aktivierte Verteilergruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Für die indirekte Zuweisung von Exchange Online E-Mail-

aktivierten Verteilergruppen prüfen Sie folgende Einstellungen und passen Sie die Einstellungen bei Bedarf an.

1. Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Identitäten und Exchange Online E-Mail-aktivierten Verteilergruppen erlaubt.

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

   Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

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

      - ODER -

      Wählen Sie im Manager in der Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.
   2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
      - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
      - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
   3. Speichern Sie die Änderungen.
2. Einstellungen für die Zuweisung von E-Mail-aktivierten Verteilergruppen zu Postfächern.
   - Das Postfach ist mit der Option **Gruppen erbbar** gekennzeichnet.
   - Das Azure Active Directory Benutzerkonto des Postfachs ist mit einer Identität verbunden.
3. Einstellungen für die Zuweisung von E-Mail-aktivierten Verteilergruppen zu E-Mail Benutzern.
   - Der E-Mail Benutzer ist mit der Option **Gruppen erbbar** gekennzeichnet.
   - Der E-Mail Benutzer ist mit einer Identität verbunden.
4. Einstellungen für die Zuweisung von E-Mail-aktivierten Verteilergruppen zu E-Mail Kontakten.
   - Der E-Mail Kontakt ist mit der Option **Gruppen erbbar** gekennzeichnet.
   - Der E-Mail Kontakt ist mit einer Identität verbunden.

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

Verwandte Themen

- Allgemeine Stammdaten für Exchange Online Postfächer auf Seite 102
- Stammdaten für Exchange Online E-Mail Benutzer auf Seite 121
- Stammdaten für Exchange Online E-Mail Kontakte auf Seite 134

Exchange Online E-Mail-aktivierte Verteilergruppen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die die E-Mail-aktivierte Verteilergruppe an Abteilungen, Kostenstellen oder Standorte zu, damit die die E-Mail-aktivierte Verteilergruppe über diese Organisationen an Postfächer, E-Mail Benutzer und E-Mail Kontakte zugewiesen wird.

Um eine die E-Mail-aktivierte Verteilergruppe an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
    - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
    - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
    - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

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

    Um eine Zuweisung zu entfernen

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

Um die E-Mail-aktivierte Verteilergruppen an eine Abteilung, eine Kostenstelle oder einen Standort zuzuweisen (bei nicht-rollenbasierter Anmeldung oder bei rollenbasierter Anmeldung)

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

    - ODER -

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

    - ODER -

Wählen Sie im Manager die Kategorie **Organisationen > Standorte**.

2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **Exchange Online E-Mail-aktivierte Verteilergruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die E-Mail-aktivierten Verteilergruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von E-Mail-aktivierten Verteilergruppen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die E-Mail-aktivierte Verteilergruppe und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Exchange Online E-Mail-aktivierten Verteilergruppen auf Seite 154
- Exchange Online E-Mail-aktivierte Verteilergruppen an Geschäftsrollen zuweisen auf Seite 157
- Exchange Online E-Mail-aktivierte Verteilergruppen in Systemrollen aufnehmen auf Seite 159
- Exchange Online E-Mail-aktivierte Verteilergruppen in den IT Shop aufnehmen auf Seite 160
- One Identity Manager Benutzer für die Verwaltung einer Exchange Online-Umgebung auf Seite 11

Exchange Online E-Mail-aktivierte Verteilergruppen an Geschäftsrollen zuweisen

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

Weisen Sie die die E-Mail-aktivierte Verteilergruppe an Geschäftsrollen zu, damit die E-Mail-aktivierte Verteilergruppe über diese Geschäftsrollen an Benutzerkonten zugewiesen wird.

Um eine E-Mail-aktivierte Verteilergruppe an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Um E-Mail-aktivierte Verteilergruppen an eine Geschäftsrolle zuzuweisen (bei nicht-rollenbasierter Anmeldung oder bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen > <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **Exchange Online E-Mail-aktivierte Verteilergruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die E-Mail-aktivierten Verteilergruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von E-Mail-aktivierten Verteilergruppen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die E-Mail-aktivierte Verteilergruppe und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Exchange Online E-Mail-aktivierten Verteilergruppen auf Seite 154
- Exchange Online E-Mail-aktivierte Verteilergruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 156
- Exchange Online E-Mail-aktivierte Verteilergruppen in Systemrollen aufnehmen auf Seite 159
- Exchange Online E-Mail-aktivierte Verteilergruppen in den IT Shop aufnehmen auf Seite 160
- One Identity Manager Benutzer für die Verwaltung einer Exchange Online-Umgebung auf Seite 11

Exchange Online E-Mail-aktivierte Verteilergruppen in Systemrollen aufnehmen

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

Mit dieser Aufgabe nehmen Sie eine Gruppe in Systemrollen auf. Wenn Sie eine Systemrolle an Identitäten zuweisen, wird die E-Mail-aktivierte Verteilergruppe an alle Postfächer, E-Mail Benutzer und E-Mail Kontakte vererbt, die diese Identitäten besitzen.

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

Um eine E-Mail-aktivierte Verteilergruppe an Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Exchange Online E-Mail-aktivierte Verteilergruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 156
- Exchange Online E-Mail-aktivierte Verteilergruppen an Geschäftsrollen zuweisen auf Seite 157
- Exchange Online E-Mail-aktivierte Verteilergruppen in den IT Shop aufnehmen auf Seite 160

Exchange Online E-Mail-aktivierte Verteilergruppen in den IT Shop aufnehmen

Mit der Zuweisung einer E-Mail-aktivierten Verteilergruppe an ein IT Shop Regal kann die E-Mail-aktivierte Verteilergruppe von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Die E-Mail-aktivierte Verteilergruppe muss mit der Option **IT Shop** gekennzeichnet sein.
- Die E-Mail-aktivierte Verteilergruppe muss eine Leistungsposition zugeordnet sein.

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die E-Mail-aktivierte Verteilergruppe im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Service-kategorie zu.
- Soll die E-Mail-aktivierte Verteilergruppe nur über IT Shop-Bestellungen an Identitäten zugewiesen werden können, muss die E-Mail-aktivierte Verteilergruppe zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen oder Postfächer, E-Mail Benutzer und E-Mail Kontakte ist dann nicht mehr zulässig.

HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren E-Mail-aktivierte Verteilergruppen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt E-Mail-aktivierte Verteilergruppen in den IT Shop aufzunehmen.

Um eine E-Mail-aktivierte Verteilergruppe in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Exchange Online Verteilergruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die E-Mail-aktivierte Verteilergruppe an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine E-Mail-aktivierte Verteilergruppe aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

Wählen Sie im Manager die Kategorie **Berechtigungen > Exchange Online Verteilergruppen** (bei rollenbasierter Anmeldung).

2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die E-Mail-aktivierte Verteilergruppe aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine E-Mail-aktivierte Verteilergruppe aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Exchange Online Verteilergruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Die E-Mail-aktivierte Verteilergruppe wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser E-Mail-aktivierten Verteilergruppe abbestellt.

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

Verwandte Themen

- Stammdaten für Exchange Online E-Mail-aktivierte Verteilergruppen auf Seite 146
- Exchange Online E-Mail-aktivierte Verteilergruppen automatisch in den IT Shop aufnehmen auf Seite 162
- Exchange Online E-Mail-aktivierte Verteilergruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 156
- Exchange Online E-Mail-aktivierte Verteilergruppen an Geschäftsrollen zuweisen auf Seite 157
- Exchange Online E-Mail-aktivierte Verteilergruppen in Systemrollen aufnehmen auf Seite 159

Exchange Online E-Mail-aktivierte Verteilergruppen automatisch in den IT Shop aufnehmen

Mit den folgenden Schritten können E-Mail-aktivierten Verteilergruppen automatisch in den IT Shop aufgenommen werden. Die Synchronisation sorgt dafür, dass die E-Mail-aktivierten Verteilergruppen in den IT Shop aufgenommen werden. Bei Bedarf können Sie die Synchronisation im Synchronization Editor sofort starten. E-Mail-aktivierten Verteilergruppen, die im One Identity Manager neu erstellt werden, werden ebenfalls automatisch in den IT Shop aufgenommen.

Um E-Mail-aktivierten Verteilergruppen automatisch in den IT Shop aufzunehmen

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | O3EDL**.
2. Um einzelne E-Mail-aktivierte Verteilergruppen nicht automatisch in den IT Shop aufzunehmen, aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | O3EDL | ExcludeList**.

   Der Konfigurationsparameter enthält eine Auflistung aller E-Mail-aktivierten Verteilergruppen, die nicht automatisch zum IT Shop zugeordnet werden sollen. Bei Bedarf können Sie die Liste erweitern. Erfassen Sie dazu im Wert des Konfigurationsparameters die Namen der Gruppen. Die Namen werden in einer Pipe (|) getrennten Liste angegeben. Reguläre Ausdrücke werden unterstützt.
3. Kompilieren Sie die Datenbank.

Die E-Mail-aktivierten Verteilergruppen werden ab diesem Zeitpunkt automatisch in den IT Shop aufgenommen.

Folgende Schritte werden bei der Aufnahme einer E-Mail-aktivierten Verteilergruppe in den IT Shop automatisch ausgeführt.

1. Es wird eine Leistungsposition für die E-Mail-aktivierten Verteilergruppe ermittelt.

   Für jede E-Mail-aktivierte Verteilergruppe wird die Leistungsposition geprüft und bei Bedarf angepasst. Die Bezeichnung der Leistungsposition entspricht der Bezeichnung der E-Mail-aktivierten Verteilergruppe.

   - Für E-Mail-aktivierte Verteilergruppen mit Leistungsposition wird die Leistungsposition angepasst.
   - E-Mail-aktivierte Verteilergruppen ohne Leitungsposition erhalten eine neue Leistungsposition.
2. Die Leistungsposition wird der Standard-Servicekategorie **Azure Active Directory Gruppen | Exchange Online Verteilergruppen** zugeordnet.
3. Es wird eine Anwendungsrolle für Produkteigner ermittelt und der Leistungsposition zugeordnet.

Die Produkteigner können Bestellungen von Mitgliedschaften in diesen E-Mail-aktivierten Verteilergruppen genehmigen. Standardmäßig wird der Administrator einer E-Mail-aktivierten Verteilergruppe als Produkteigner ermittelt.

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

- Ist der Administrator der E-Mail-aktivierten Verteilergruppe bereits Mitglied einer Anwendungsrolle für Produkteigner, dann wird diese Anwendungsrolle der Leistungsposition zugewiesen. Alle Mitglieder dieser Anwendungsrolle werden dadurch Produkteigner der E-Mail-aktivierten Verteilergruppe.
- Ist der Administrator der E-Mail-aktivierten Verteilergruppe noch kein Mitglied einer Anwendungsrolle für Produkteigner, dann wird eine neue Anwendungsrolle erzeugt. Die Bezeichnung der Anwendungsrolle entspricht der Bezeichnung des Eigentümers.
  - Handelt es sich beim Administrator um ein Benutzerkonto, wird die Identität des Benutzerkontos in die Anwendungsrolle aufgenommen.
  - Handelt es sich um eine Gruppe von Administratoren, werden die Identitäten aller Benutzerkonten dieser Gruppe in die Anwendungsrolle aufgenommen.

4. Die E-Mail-aktivierte Verteilergruppe wird mit der Option **IT Shop** gekennzeichnet und dem IT Shop Regal **Exchange Online Verteilerguppen** im Shop **Identity & Access Lifecycle** zugewiesen.

Anschließend können die Kunden des Shops Mitgliedschaften in E-Mail-aktivierten Verteilergruppen über das Web Portal bestellen.

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

Ausführliche Informationen zur Konfiguration des IT Shops finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*. Ausführliche Informationen zum Bestellen von Zugriffsanforderungen im Web Portal finden Sie im *One Identity Manager Web Portal Anwenderhandbuch*.

Verwandte Themen

- Exchange Online E-Mail-aktivierte Verteilergruppen in den IT Shop aufnehmen auf Seite 160
- Exchange Online E-Mail-aktivierte Verteilergruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 156
- Exchange Online E-Mail-aktivierte Verteilergruppen an Geschäftsrollen zuweisen auf Seite 157
- Exchange Online E-Mail-aktivierte Verteilergruppen in Systemrollen aufnehmen auf Seite 159
- Exchange Online Empfänger direkt an Exchange Online E-Mail-aktivierte Verteilergruppen zuweisen auf Seite 164

- Exchange Online E-Mail-aktivierte Verteilergruppen in Exchange Online E-Mail-aktivierte Verteilergruppen aufnehmen auf Seite 168
- Administratoren für Exchange Online E-Mail-aktivierte Verteilergruppen festlegen auf Seite 152

Exchange Online Empfänger direkt an Exchange Online E-Mail-aktivierte Verteilergruppen zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die E-Mail-aktivierten Verteilergruppen direkt an Postfächer, E-Mail Benutzer und E-Mail Kontakte zuweisen. E-Mail-aktivierte Verteilergruppen, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Um Postfächer, E-Mail Benutzer und E-Mail Kontakte direkt an eine E-Mail-aktivierte Verteilergruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **Mitglieder zuweisen**.
4. Um Postfächer zuzuweisen, wählen Sie den Tabreiter **Postfächer**.

   - ODER -

   Um E-Mail Benutzer zuzuweisen, wählen Sie den Tabreiter **E-Mail Benutzer**.

   - ODER -

   Um E-Mail Kontakte zuzuweisen, wählen Sie den Tabreiter **E-Mail Kontakte**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Postfächer, E-Mail Benutzer oder E-Mail Kontakte zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Postfächern, E-Mail Benutzern oder E-Mail Kontakten entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Postfach, den E-Mail Benutzer oder den E-Mail Kontakt und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online E-Mail-aktivierte Verteilergruppen direkt an Exchange Online Postfächer zuweisen auf Seite 165

- Exchange Online E-Mail-aktivierte Verteilergruppen direkt an Exchange Online E-Mail Benutzer zuweisen auf Seite 165
- Exchange Online E-Mail-aktivierte Verteilergruppen direkt an Exchange Online E-Mail Kontakte zuweisen auf Seite 166

Exchange Online E-Mail-aktivierte Verteilergruppen direkt an Exchange Online Postfächer zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die E-Mail-aktivierten Verteilergruppen direkt an Postfächer zuweisen.

Um E-Mail-aktivierte Verteilergruppen direkt an ein Postfach zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Postfächer**.
2. Wählen Sie in der Ergebnisliste das Postfach.
3. Wählen Sie die Aufgabe **E-Mail-aktivierte Verteilergruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die E-Mail-aktivierten Verteilergruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von E-Mail-aktivierten Verteilergruppen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die E-Mail-aktivierte Verteilergruppe und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online Empfänger direkt an Exchange Online E-Mail-aktivierte Verteilergruppen zuweisen auf Seite 164

Exchange Online E-Mail-aktivierte Verteilergruppen direkt an Exchange Online E-Mail Benutzer zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die E-Mail-aktivierten Verteilergruppen direkt an E-Mail Benutzer zuweisen.

Um E-Mail-aktivierte Verteilergruppen direkt an einen E-Mail Benutzer zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Benutzer**.
2. Wählen Sie in der Ergebnisliste den E-Mail Benutzer.
3. Wählen Sie die Aufgabe **E-Mail-aktivierte Verteilergruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die E-Mail-aktivierten Verteilergruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von E-Mail-aktivierten Verteilergruppen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die E-Mail-aktivierte Verteilergruppe und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online Empfänger direkt an Exchange Online E-Mail-aktivierte Verteilergruppen zuweisen auf Seite 164

Exchange Online E-Mail-aktivierte Verteilergruppen direkt an Exchange Online E-Mail Kontakte zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die E-Mail-aktivierten Verteilergruppen direkt an E-Mail Kontakte zuweisen.

Um E-Mail-aktivierte Verteilergruppen direkt an einen E-Mail Kontakt zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail Kontakte**.
2. Wählen Sie in der Ergebnisliste den E-Mail Kontakt.
3. Wählen Sie die Aufgabe **E-Mail-aktivierte Verteilergruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die E-Mail-aktivierten Verteilergruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von E-Mail-aktivierten Verteilergruppen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die E-Mail-aktivierte Verteilergruppe und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online Empfänger direkt an Exchange Online E-Mail-aktivierte Verteilergruppen zuweisen auf Seite 164

Vererbung von Exchange Online E-Mail-aktivierten Verteilergruppen anhand von Kategorien

Für Exchange Online kann die Vererbung von Mail-aktivierten Verteilergruppen an Postfächer, E-Mail Benutzer und E-Mail Kontakte über Kategorien genutzt werden.

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

Um die Vererbung über Kategorien zu nutzen

1. Definieren Sie im Manager am Azure Active Directory Mandanten die Kategorien.

   Um die Stammdaten eines Azure Active Directory Mandanten zu bearbeiten

   1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten**.
   2. Wählen Sie in der Ergebnisliste den Azure Active Directory Mandanten.
   3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
   4. Bearbeiten Sie die Stammdaten für einen Azure Active Directory Mandanten.
   5. Speichern Sie die Änderungen.
2. Weisen Sie im Manager die Kategorien den Postfächern, E-Mail Benutzern und E-Mail Kontakten über ihre Stammdaten zu.
3. Weisen Sie im Manager die Kategorien den E-Mail-aktivierten Verteilergruppen über ihre Stammdaten zu.

Verwandte Themen

- Allgemeine Stammdaten für Exchange Online Postfächer auf Seite 102
- Stammdaten für Exchange Online E-Mail Benutzer auf Seite 121
- Stammdaten für Exchange Online E-Mail Kontakte auf Seite 134
- Stammdaten für Exchange Online E-Mail-aktivierte Verteilergruppen auf Seite 146

Exchange Online E-Mail-aktivierte Verteilergruppen in Exchange Online E-Mail-aktivierte Verteilergruppen aufnehmen

Um E-Mail-aktivierte Verteilergruppen in eine E-Mail-aktivierte Verteilergruppe aufzunehmen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **E-Mail-aktivierte Verteilergruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die E-Mail-aktivierten Verteilergruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von E-Mail-aktivierten Verteilergruppen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die E-Mail-aktivierte Verteilergruppe und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Exchange Online dynamische Verteilergruppen in Exchange Online E-Mail-aktivierte Verteilergruppen aufnehmen

Um dynamische Verteilergruppen in eine E-Mail-aktivierte Verteilergruppe aufzunehmen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **Mitglieder zuweisen**.
4. Wählen Sie den Tabreiter **Dynamische Verteilergruppen**.

5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die dynamischen Verteilergruppen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die dynamische Verteilergruppe und doppelklicken Sie ✓.

6. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online E-Mail-aktivierte Verteilergruppen in Exchange Online dynamische Verteilergruppen aufnehmen auf Seite 200

Exchange Online E-Mail-aktivierte öffentliche Ordner an Exchange Online E-Mail-aktivierte Verteilergruppen zuweisen

Um E-Mail-aktivierte öffentliche Ordner an eine E-Mail-aktivierte Verteilergruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **E-Mail-aktivierte öffentliche Ordner zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die E-Mail-aktivierten öffentliche Ordner zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von E-Mail-aktivierten öffentliche Ordnern entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie den E-Mail-aktivierte öffentlichen Ordner und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Zusatzeigenschaften an Exchange Online E-Mail-aktivierte Verteilergruppen zuweisen

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

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

Um Zusatzeigenschaften für eine E-Mail-aktivierte Verteilergruppe festzulegen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

Exchange Online E-Mail-aktivierte Verteilergruppen löschen

Beim Löschen einer E-Mail-aktivierten Verteilergruppe wird zusätzlich die Azure Active Directory Gruppe, die mit der E-Mail-aktivierten Verteilergruppe verknüpft ist, gelöscht.

Um eine E-Mail-aktivierte Verteilergruppe zu löschen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > E-Mail-aktivierte Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die E-Mail-aktivierte Verteilergruppe.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Exchange Online Office 365 Gruppen

Office 365 Gruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können Office 365 Gruppen im One Identity Manager erstellen und bearbeiten. Beim Erzeugen einer Office 365 Gruppe wird zusätzlich eine Azure Active Directory Gruppe erzeugt und mit der Office 365 Gruppe verknüpft.

Im One Identity Manager können Sie die Office 365 Gruppen direkt an die Postfächer, E-Mail Benutzer und E-Mail Kontakte zuweisen oder über Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen vererben. Des Weiteren können Benutzer die Office 365 Gruppen über das Web Portal bestellen. Dazu werden die Office 365 Gruppen im IT Shop bereitgestellt.

Detaillierte Informationen zum Thema

- Exchange Online Office 365 Gruppen erstellen auf Seite 172
- Stammdaten für Exchange Online Office 365 Gruppen bearbeiten auf Seite 172
- Stammdaten für Exchange Online Office 365 Gruppen auf Seite 173
- Empfangsbeschränkungen für Exchange Online Office 365 Gruppen anpassen auf Seite 177
- Eigentümer an Exchange Online Office 365 Gruppen zuweisen auf Seite 178
- Abonnenten an Exchange Online Office 365 Gruppen zuweisen auf Seite 178
- Zuweisen von Exchange Online Office 365 Gruppen an Azure Active Directory Benutzerkonten auf Seite 179
- Vererbung von Exchange Online Office 365 Gruppen anhand von Kategorien auf Seite 191
- Zusatzeigenschaften an Exchange Online Office 365 Gruppen zuweisen auf Seite 192
- Exchange Online Office 365 Gruppen löschen auf Seite 193
- Einzelobjekte synchronisieren auf Seite 53

Exchange Online Office 365 Gruppen erstellen

Beim Erzeugen einer Office 365 Gruppe wird zusätzlich eine Azure Active Directory Gruppe erzeugt und mit der Office 365 Gruppe verknüpft.

Um eine Office 365 Gruppe zu erstellen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular erfassen Sie die Stammdaten der Office 365 Gruppe.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Exchange Online Office 365 Gruppen bearbeiten auf Seite 172
- Stammdaten für Exchange Online Office 365 Gruppen auf Seite 173

Stammdaten für Exchange Online Office 365 Gruppen bearbeiten

Um eine Office 365 Gruppe zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen**.
2. Wählen Sie in der Ergebnisliste die Office 365 Gruppe und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten der Office 365 Gruppe.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online Office 365 Gruppen erstellen auf Seite 172
- Stammdaten für Exchange Online Office 365 Gruppen auf Seite 173

Stammdaten für Exchange Online Office 365 Gruppen

Tabelle 20: Stammdaten einer Exchange Online Gruppe

Eigenschaft	Beschreibung
Azure Active Directory Mandant	Bezeichnung des Azure Active Directory Mandanten.
Bezeichnung	Bezeichnung der Office 365 Gruppe.
Anzeigename	Anzeigename, wie er im Adressbuch verwendet wird.
Einfache Anzeige	Einfacher Anzeigename für Systeme, die nicht alle Zeichen des normalen Anzeigenamens interpretieren können.
Alias	Eindeutiger Alias zur weiteren Identifizierung der Office 365 Gruppe.
Gruppentyp	Typ der Gruppe.
Proxy Adressen	E-Mail-Adressen zur Office 365 Gruppe. Als Adresstyp können Sie zusätzlich zur Standardadressierung (SMTP, X400) weitere Mailkonnektoren (beispielsweise CCMail, MS) nutzen. Für die Erstellung weiterer Proxyadressen ist die folgende Syntax einzuhalten: `Adresstyp: neue E-Mail-Adresse`
Yammer E-Mail Adresse	Yammer E-Mail Adresse.
Notizen	Weitere Informationen zur Office 365 Gruppe.
Azure Active Directory Gruppe	Azure Active Directory Gruppe, für welche eine Office 365 Gruppe erzeugt wird.
IT Shop	Gibt an, ob die Gruppe über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Postfächer, E-Mail Benutzer und E-Mail Kontakte und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert,

Eigenschaft	Beschreibung
	kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Postfächer, E-Mail Benutzer und E-Mail Kontakte ist nicht zulässig.
Leistungsposition	Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Postfächer, E-Mail Benutzer und E-Mail Kontakte. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen zur Risikobewertung finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen an Postfächer, E-Mail Benutzer und E-Mail Kontakte. Gruppen können selektiv an die Postfächer, E-Mail Benutzer und E-Mail Kontakte vererbt werden. Dazu werden die Gruppen und die Postfächer, E-Mail Benutzer und E-Mail Kontakte in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Datenschutz	Datenschutztyp für die Office 365 Gruppe. Zur Auswahl stehen **Privat** (Standard) oder **Öffentlich**.
Sprache	Sprache der Office 365 Gruppe.
Klassifizierung	Klassifizierung der Office 365 Gruppe.
Nicht in Adresslisten anzeigen	Gibt an, ob die Office 365 Gruppe in Adressbüchern angezeigt werden soll. Setzen Sie die Option, wenn Sie verhindern wollen, dass die Office 365 Gruppe in Adressbüchern angezeigt wird. Diese Option gilt für die Anzeige in allen Adressbüchern.
Gruppenmitgliedschaften nicht anzeigen	Gibt an, ob die Mitglieder der Office 365 Gruppe

Eigenschaft	Beschreibung
	für Benutzer ausgeblendet werden, die keine Mitglieder der Gruppe sind. Die Option kann nur für private Gruppen aktiviert werden.
Gruppe in Outlook ausblenden	Gibt an, ob die Office 365 Gruppe in Outlook angezeigt werden soll. Setzen Sie die Option, wenn Sie verhindern wollen, dass die Office 365 Gruppe in Outlook angezeigt wird. Die Office 365 Gruppe wird ebenfalls in Adressbüchern ausgeblendet.
Exchange Version	Angabe der Exchange Version.
Postfach konfiguriert	Gibt an, ob ein Postfach für die Office 365 Gruppe konfiguriert wurde.
Posteingang URL	URL des Posteingangs.
Max. Sendegröße [KB]	Maximale Sendegröße von Nachrichten in KB.
Absender-Authenfizierung erforderlich	Gibt an, ob die Authentifizierungsinformationen von Absendern angefordert werden. Setzen Sie die Option, um zu verhindern, dass anonyme Absender Benachrichtigungen an die Office 365 Gruppe senden können.
Einschränkungen zur Postfach-bereitstellung	Zusätzliche Optionen zur Postfachbereitstellung.
E-Mail-Info	Benutzerdefinierte E-Mail-Info-Text für diesen Empfänger.
E-Mail-Info Übersetzungen	Sprachen für den benutzerdefinierten E-Mail-Info-Text.
Willkommensnachricht aktiviert	Gibt an, ob eine Willkommensnachricht gesendet wird.
Migration zu Office 365 Gruppe läuft	Angabe des Migrationsstatus.
Gültig	Gibt an, ob diese Office 365 Gruppe gültig ist.
Dynamische Mitgliedschaft	Gibt an, ob die Mitgliedschaften dynamisch sind.
Hinzufügen von neuen Gästen erlaubt	Gibt an, ob neue Gäste zur Office 365 Gruppe hinzugefügt werden können.
Anzahl externer Mitglieder	Anzahl der externe Gruppenmitglieder.
Abonnements zulassen	Gibt an, ob Abonnements für Unterhaltungen und Kalenderereignisse für die Office 365 Gruppe aktiviert werden. Abonnenten

Eigenschaft	Beschreibung
	weisen Sie über die Aufgabe **Abonnements zuweisen** zu.
Neue Mitglieder automatisch abonnieren	Gibt an, ob für neue Mitglieder, die zur Office 365 Gruppe hinzugefügt werden, automatisch ein Abonnement für Unterhaltungen und Kalenderereignisse erstellt wird.
Mitglieder nur für Kalenderereignisse abonnieren	Gibt an, ob für die Mitglieder der Office 365 Gruppe nur Gruppenkalenderereignisse und keine Unterhaltungen abonniert werden.
Externe Ressourcen publiziert	Gibt an, ob externe Ressourcen publiziert werden.
Konnektoren zulassen	Gibt an, ob die Möglichkeit zur Verwendung von Konnektoren für Apps, Tools oder Dienste für die Office 365 Gruppe aktiviert wird.
Synchronisiert mit dem lokalen Active Directory	Gibt an, ob die Gruppe im lokalen Active Directory erstellt und mit Exchange Online synchronisiert wurde.
Dateibenachrichtigungseinstellungen	Einstellungen für Dateibenachrichtigungen.
Identität URL	URL der Identität.
Foto URL	URL des Fotos.
SharePoint Dokumente URL	URL für SharePoint Dokumente.
SharePoint Notizbuch URL	URL für das SharePoint Notizbuch.
SharePoint Website URL	URL für die SharePoint Website.
Benutzerdefiniertes Attribut 01 - Benutzerdefiniertes Attribut 15	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Attributerweiterung 01 - Attributerweiterung 15	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Verwandte Themen

- Abonnenten an Exchange Online Office 365 Gruppen zuweisen auf Seite 178

Empfangsbeschränkungen für Exchange Online Office 365 Gruppen anpassen

HINWEIS: Die Zuweisungen **Postannahme erlauben** und **Postannahme verweigern** schließen einander aus. Sie können entweder festlegen, ob die Nachrichten eines Empfängers akzeptiert werden oder abgelehnt werden.

Um die Postannahme für Office 365 Gruppen anzupassen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen**.
2. Wählen Sie in der Ergebnisliste die Office 365 Gruppe.
3. Wählen Sie die Aufgabe **Postannahme erlauben**, um festzulegen, von welchen Empfängern Nachrichten akzeptiert werden.

   - ODER -

   Wählen Sie die Aufgabe **Postannahme verweigern**, um festzulegen, von welchen Empfängern Nachrichten abgelehnt werden.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Empfänger enthält. Zur Auswahl stehen:
   - E-Mail-aktivierte Verteilergruppen
   - Dynamische Verteilergruppen
   - Postfächer
   - E-Mail Benutzer
   - E-Mail Kontakte
   - Office 365 Gruppen
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Empfänger zu.

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

   Um eine Zuweisung zu entfernen
   - Wählen Sie den Empfänger und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Eigentümer an Exchange Online Office 365 Gruppen zuweisen

Wenn Sie Eigentümer an eine Office 365 Gruppe zuweisen, werden diese Eigentümer zusätzlich als Mitglieder in die Office 365 Gruppe aufgenommen.

HINWEIS: Eigentümer können nicht manuell an dynamische Office 365 Gruppen zugewiesen werden.

Um Eigentümer an eine Office 365 Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen**.
2. Wählen Sie in der Ergebnisliste die Office 365 Gruppe.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Eigentümer zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Eigentümer und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- Azure Active Directory Benutzerkonten direkt an Exchange Online Office 365 Gruppen zuweisen auf Seite 190

Abonnenten an Exchange Online Office 365 Gruppen zuweisen

Abonnenten können Sie an Office 365 Gruppen zuweisen, wenn für die Gruppe die Option **Abonnements zulassen** aktiviert ist. Wenn Sie Abonnenten an eine Office 365 Gruppe zuweisen, werden diese Abonnenten zusätzlich als Mitglieder in die Office 365 Gruppe aufgenommen.

HINWEIS: Abonnenten können nicht manuell an dynamische Office 365 Gruppen zugewiesen werden.

Um Abonnenten an eine Office 365 Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen**.
2. Wählen Sie in der Ergebnisliste die Office 365 Gruppe.
3. Wählen Sie die Aufgabe **Abonnenten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Abonnenten zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Abonnent und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Exchange Online Office 365 Gruppen auf Seite 173
- Stammdaten für Exchange Online Office 365 Gruppen bearbeiten auf Seite 172
- Azure Active Directory Benutzerkonten direkt an Exchange Online Office 365 Gruppen zuweisen auf Seite 190

Zuweisen von Exchange Online Office 365 Gruppen an Azure Active Directory Benutzerkonten

Office 365 Gruppen können indirekt oder direkt an Azure Active Directory Benutzerkonten zugewiesen werden.

Bei der indirekten Zuweisung werden Identitäten und Office 365 Gruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die Office 365 Gruppen berechnet, die einer Identität zugewiesen sind. Wenn Sie eine Identität in Rollen aufnehmen und die Identität ein Azure Active Directory Benutzerkonto besitzt, dann wird dieses Azure Active Directory Benutzerkonto in die Office 365 Gruppen aufgenommen.

Des Weiteren können Office 365 Gruppen im Web Portal bestellt werden. Dazu werden Identitäten als Kunden in einen Shop aufgenommen. Alle Office 365 Gruppen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Office 365 Gruppen werden nach erfolgreicher Genehmigung den Identitäten zugewiesen.

Über Systemrollen können Office 365 Gruppen zusammengefasst und als Paket an Identitäten und Arbeitsplätze zugewiesen werden. Sie können Systemrollen erstellen, die ausschließlich Office 365 Gruppen enthalten. Ebenso können Sie in einer Systemrolle beliebige Unternehmensressourcen zusammenfassen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Office 365 Gruppen auch direkt an Azure Active Directory Benutzerkonten zuweisen.

Ausführliche Informationen finden Sie in den folgenden Handbüchern.

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

Detaillierte Informationen zum Thema

- Voraussetzungen für indirekte Zuweisungen von Office 365 Gruppen an die Azure Active Directory Benutzerkonten auf Seite 180
- Exchange Online Office 365 Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 182
- Exchange Online Office 365 Gruppen an Geschäftsrollen zuweisen auf Seite 183
- Exchange Online Office 365 Gruppen in Systemrollen aufnehmen auf Seite 185
- Exchange Online Office 365 Gruppen in den IT Shop aufnehmen auf Seite 186
- Exchange Online Office 365 Gruppen automatisch in den IT Shop aufnehmen auf Seite 187
- Azure Active Directory Benutzerkonten direkt an Exchange Online Office 365 Gruppen zuweisen auf Seite 190
- Exchange Online Office 365 Gruppen direkt an Azure Active Directory Benutzerkonten zuweisen auf Seite 189

Voraussetzungen für indirekte Zuweisungen von Office 365 Gruppen an die Azure Active Directory Benutzerkonten

Bei der indirekten Zuweisung werden Identitäten und Office 365 Gruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Für die indirekte Zuweisung von Office 365 Gruppen prüfen Sie folgende Einstellungen und passen Sie die Einstellungen bei Bedarf an.

1. Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Identitäten und Exchange Online Office 365 Gruppen erlaubt.

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

   Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

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

      - ODER -

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

2. Einstellungen für die Zuweisung von Office 365 Gruppen an Azure Active Directory Benutzerkonten.
   - Das Azure Active Directory Benutzerkonto ist mit einer Identität verbunden.
   - Am Azure Active Directory Benutzerkonto ist die Option **Office 365 Gruppen erbbar** aktiviert.

     Die Option gibt an, ob das Azure Active Directory Benutzerkonto Office 365 Gruppen über die verbundene Identität erben darf. Ist die Option aktiviert, werden Office 365 Gruppen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt.
     - Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Office 365 Gruppen zugewiesen haben, dann erbt das Azure Active Directory Benutzerkonto diese Office 365 Gruppen.
     - Wenn eine Identität eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Azure Active Directory Benutzerkonto der Identität diese Office 365 Gruppe nur, wenn die Option aktiviert ist.

   Um die Stammdaten eines Benutzerkontos zu bearbeiten

   1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Benutzerkonten**.
   2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
   3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

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

Ausführliche Informationen zu Azure Active Directory Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung*.

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

Exchange Online Office 365 Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen

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

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

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

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

   Um eine Zuweisung zu entfernen

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

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

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

   - ODER -

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

   - ODER -

   Wählen Sie im Manager die Kategorie **Organisationen > Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **Office 365 Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Office 365 Gruppen an die Azure Active Directory Benutzerkonten auf Seite 180
- Exchange Online Office 365 Gruppen an Geschäftsrollen zuweisen auf Seite 183
- Exchange Online Office 365 Gruppen in Systemrollen aufnehmen auf Seite 185
- Exchange Online Office 365 Gruppen in den IT Shop aufnehmen auf Seite 186
- One Identity Manager Benutzer für die Verwaltung einer Exchange Online-Umgebung auf Seite 11

Exchange Online Office 365 Gruppen an Geschäftsrollen zuweisen

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

Weisen Sie die Gruppe an Geschäftsrollen zu, damit die Gruppe über diese Geschäftsrollen an Benutzerkonten zugewiesen wird.

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

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen an eine Geschäftsrolle zuzuweisen (bei nicht-rollenbasierter Anmeldung oder bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen > <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **Office 365 Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Office 365 Gruppen an die Azure Active Directory Benutzerkonten auf Seite 180
- Exchange Online Office 365 Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 182
- Exchange Online Office 365 Gruppen in Systemrollen aufnehmen auf Seite 185
- Exchange Online Office 365 Gruppen in den IT Shop aufnehmen auf Seite 186
- One Identity Manager Benutzer für die Verwaltung einer Exchange Online-Umgebung auf Seite 11

Exchange Online Office 365 Gruppen in Systemrollen aufnehmen

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

Mit dieser Aufgabe nehmen Sie eine Gruppe in Systemrollen auf.

Wenn Sie eine Systemrolle an Identitäten zuweisen, wird die Gruppe an alle Azure Active Directory Benutzerkonten vererbt, die diese Identitäten besitzen.

Diese Aufgabe steht für dynamische Gruppen nicht zur Verfügung.

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

Um eine Gruppe an Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Office 365 Gruppen an die Azure Active Directory Benutzerkonten auf Seite 180
- Exchange Online Office 365 Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 182
- Exchange Online Office 365 Gruppen an Geschäftsrollen zuweisen auf Seite 183
- Exchange Online Office 365 Gruppen in den IT Shop aufnehmen auf Seite 186

Exchange Online Office 365 Gruppen in den IT Shop aufnehmen

Mit der Zuweisung einer Office 365 Gruppe an ein IT Shop Regal kann die Office 365 Gruppe von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Die Gruppe ist keine dynamische Gruppe.
- Die Office 365 Gruppe muss mit der Option **IT Shop** gekennzeichnet sein.
- Die Office 365 Gruppe muss eine Leistungsposition zugeordnet sein.

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Office 365 Gruppe im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.
- Soll die Office 365 Gruppe nur über IT Shop-Bestellungen an Identitäten zugewiesen werden können, muss die Office 365 Gruppe zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen oder Active Directory Benutzerkonten ist dann nicht mehr zulässig.

HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren Office 365 Gruppen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Office 365 Gruppen in den IT Shop aufzunehmen.

Um eine Office 365 Gruppe in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Office 365 Gruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Office 365 Gruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Office 365 Gruppe an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Office 365 Gruppe aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Office 365 Gruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Office 365 Gruppe.

3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Office 365 Gruppe aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Office 365 Gruppe aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Office 365 Gruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Office 365 Gruppe.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Die Office 365 Gruppe wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieserOffice 365 Gruppe abbestellt.

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

Verwandte Themen

- Stammdaten für Exchange Online Office 365 Gruppen auf Seite 173
- Voraussetzungen für indirekte Zuweisungen von Office 365 Gruppen an die Azure Active Directory Benutzerkonten auf Seite 180
- Exchange Online Office 365 Gruppen automatisch in den IT Shop aufnehmen auf Seite 187
- Exchange Online Office 365 Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 182
- Exchange Online Office 365 Gruppen an Geschäftsrollen zuweisen auf Seite 183
- Exchange Online Office 365 Gruppen in Systemrollen aufnehmen auf Seite 185

Exchange Online Office 365 Gruppen automatisch in den IT Shop aufnehmen

Mit den folgenden Schritten können Exchange Online Office 365 Gruppen automatisch in den IT Shop aufgenommen werden. Die Synchronisation sorgt dafür, dass die Office 365 Gruppen in den IT Shop aufgenommen werden. Bei Bedarf können Sie die Synchronisation

im Synchronization Editor sofort starten. Office 365 Gruppen, die im One Identity Manager neu erstellt werden, werden ebenfalls automatisch in den IT Shop aufgenommen.

Um Office 365 Gruppen automatisch in den IT Shop aufzunehmen

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | O3EUnifiedGroup**.
2. Um einzelne Office 365 Gruppen nicht automatisch in den IT Shop aufzunehmen, aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | O3EUnifiedGroup | ExcludeList**.

   Der Konfigurationsparameter enthält eine Auflistung aller Office 365 Gruppen, die nicht automatisch zum IT Shop zugeordnet werden sollen. Bei Bedarf können Sie die Liste erweitern. Erfassen Sie dazu im Wert des Konfigurationsparameters die Namen der Gruppen. Die Namen werden in einer Pipe (|) getrennten Liste angegeben. Reguläre Ausdrücke werden unterstützt.
3. Kompilieren Sie die Datenbank.

Die Office 365 Gruppen werden ab diesem Zeitpunkt automatisch in den IT Shop aufgenommen.

Folgende Schritte werden bei der Aufnahme einer Office 365 Gruppe in den IT Shop automatisch ausgeführt.

1. Es wird eine Leistungsposition für die Office 365 Gruppe ermittelt.

   Für jede Office 365 Gruppe wird die Leistungsposition geprüft und bei Bedarf angepasst. Die Bezeichnung der Leistungsposition entspricht der Bezeichnung der Office 365 Gruppe.

   - Für Office 365 Gruppen mit Leistungsposition wird die Leistungsposition angepasst.
   - Office 365 Gruppen ohne Leitungsposition erhalten eine neue Leistungsposition.
2. Die Leistungsposition wird der Standard-Servicekategorie **Azure Active Directory Gruppen | Office 365 Gruppen** zugeordnet.
3. Es wird eine Anwendungsrolle für Produkteigner ermittelt und der Leistungsposition zugeordnet.

   Die Produkteigner können Bestellungen von Mitgliedschaften in diesen Office 365 Gruppen genehmigen. Standardmäßig wird der Eigentümer einer Office 365 Gruppe als Produkteigner ermittelt.

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

   - Ist der Eigentümer der Office 365 Gruppe bereits Mitglied einer Anwendungsrolle für Produkteigner, dann wird diese Anwendungsrolle der Leistungsposition zugewiesen. Alle Mitglieder dieser Anwendungsrolle werden dadurch Produkteigner der Azure Active Directory Gruppe.

- Ist der Eigentümer der Office 365 Gruppe noch kein Mitglied einer Anwendungsrolle für Produkteigner, dann wird eine neue Anwendungsrolle erzeugt. Die Bezeichnung der Anwendungsrolle entspricht der Bezeichnung des Eigentümers.
    - Handelt es sich beim Eigentümer um ein Benutzerkonto, wird die Identität des Benutzerkontos in die Anwendungsrolle aufgenommen.
    - Handelt es sich um eine Gruppe von Eigentümern, werden die Identitäten aller Benutzerkonten dieser Gruppe in die Anwendungsrolle aufgenommen.

4. Die Office 365 Gruppe wird mit der Option **IT Shop** gekennzeichnet und dem IT Shop Regal **Office 365 Gruppen** im Shop **Identity & Access Lifecycle** zugewiesen.

Anschließend können die Kunden des Shops Mitgliedschaften in Office 365 Gruppen über das Web Portal bestellen.

HINWEIS: Wenn eine Office 365 Gruppe endgültig aus der One Identity Manager-Datenbank gelöscht wird, wird auch die zugehörige Leistungsposition gelöscht.

Ausführliche Informationen zur Konfiguration des IT Shops finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*. Ausführliche Informationen zum Bestellen von Zugriffsanforderungen im Web Portal finden Sie im *One Identity Manager Web Portal Anwenderhandbuch*.

Verwandte Themen

- Exchange Online Office 365 Gruppen in den IT Shop aufnehmen auf Seite 186
- Exchange Online Office 365 Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 182
- Exchange Online Office 365 Gruppen an Geschäftsrollen zuweisen auf Seite 183
- Exchange Online Office 365 Gruppen in Systemrollen aufnehmen auf Seite 185
- Azure Active Directory Benutzerkonten direkt an Exchange Online Office 365 Gruppen zuweisen auf Seite 190

Exchange Online Office 365 Gruppen direkt an Azure Active Directory Benutzerkonten zuweisen

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

Um Gruppen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Office 365 Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Azure Active Directory Benutzerkonten direkt an Exchange Online Office 365 Gruppen zuweisen auf Seite 190

Azure Active Directory Benutzerkonten direkt an Exchange Online Office 365 Gruppen zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Gruppe direkt an Benutzerkonten zuweisen. Gruppen, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Wenn Sie Eigentümer und Abonnenten an eine Office 365 Gruppe zuweisen, werden diese Benutzerkonten zusätzlich als Mitglieder in die Office 365 Gruppe aufgenommen.

HINWEIS: Benutzerkonten können nicht manuell in dynamische Office 365 Gruppen aufgenommen werden.

Um Benutzerkonten direkt an eine Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen**.
2. Wählen Sie in der Ergebnisliste die Office 365 Gruppe.
3. Wählen Sie die Aufgabe **Mitglieder zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie das Benutzerkonto und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online Office 365 Gruppen direkt an Azure Active Directory Benutzerkonten zuweisen auf Seite 189
- Eigentümer an Exchange Online Office 365 Gruppen zuweisen auf Seite 178
- Abonnenten an Exchange Online Office 365 Gruppen zuweisen auf Seite 178

Vererbung von Exchange Online Office 365 Gruppen anhand von Kategorien

Für Exchange Online kann die Vererbung von Office 365 Gruppen an Azure Active Directory Benutzerkonten über Kategorien genutzt werden.

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

Um die Vererbung über Kategorien zu nutzen

1. Definieren Sie im Manager am Azure Active Directory Mandanten die Kategorien.

   Um die Stammdaten eines Azure Active Directory Mandanten zu bearbeiten

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

2. Weisen Sie im Manager die Kategorien den Azure Active Directory Benutzerkonten über ihre Stammdaten zu.

   Um die Stammdaten eines Benutzerkontos zu bearbeiten

   1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Benutzerkonten**.
   2. Wählen Sie in der Ergebnisliste das Benutzerkonto.

3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Benutzerkontos.
5. Speichern Sie die Änderungen.

3. Weisen Sie im Manager die Kategorien den Office 365 Gruppen über ihre Stammdaten zu.

Verwandte Themen

- Stammdaten für Exchange Online Office 365 Gruppen auf Seite 173

Zusatzeigenschaften an Exchange Online Office 365 Gruppen zuweisen

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

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

Um Zusatzeigenschaften für eine Office 365 Gruppe festzulegen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen**.
2. Wählen Sie in der Ergebnisliste die Office 365 Gruppe.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

Exchange Online Office 365 Gruppen löschen

Beim Löschen einer Office 365 Gruppe wird zusätzlich die Azure Active Directory Gruppe, die mit der Office 365 Gruppe verknüpft ist, gelöscht.

Um eine Office 365 Gruppe zu löschen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen**.
2. Wählen Sie in der Ergebnisliste die Office 365 Gruppe.
3. Klicken Sie in der Ergebnisliste  .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

11

Exchange Online dynamische Verteilergruppen

Die Mitglieder einer dynamischen Verteilergruppe werden nicht fest zugewiesen, sondern über Filterkriterien ermittelt. Dynamische Verteilergruppen werden durch die Synchronisation in den One Identity Manager eingelesen und sind im One Identity Manager nur begrenzt bearbeitbar. Neue dynamische Verteilergruppen können Sie im One Identity Manager nicht erstellen.

Detaillierte Informationen zum Thema

- Stammdaten für Exchange Online dynamische Verteilergruppen bearbeiten auf Seite 195
- Stammdaten für Exchange Online dynamische Verteilergruppen auf Seite 195
- Empfangsbeschränkungen für Exchange Online dynamische Verteilergruppen anpassen auf Seite 197
- Sendeberechtigungen für Exchange Online dynamische Verteilergruppen anpassen auf Seite 198
- Moderatoren für Exchange Online dynamische Verteilergruppen festlegen auf Seite 199
- Exchange Online E-Mail-aktivierte Verteilergruppen in Exchange Online dynamische Verteilergruppen aufnehmen auf Seite 200
- Exchange Online dynamische Verteilergruppen löschen auf Seite 200
- Einzelobjekte synchronisieren auf Seite 53

Stammdaten für Exchange Online dynamische Verteilergruppen bearbeiten

Um die Stammdaten einer dynamischen Verteilergruppe zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten > <Azure Active Directory Mandant> > Exchange Online Administration > Empfängerkonfiguration > Dynamische Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Verteilergruppe und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten der dynamischen Verteilergruppe.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Exchange Online dynamische Verteilergruppen auf Seite 195

Stammdaten für Exchange Online dynamische Verteilergruppen

Tabelle 21: Stammdaten einer dynamischen Verteilergruppe

Eigenschaft	Beschreibung
Azure Active Directory Mandant	Bezeichnung des Azure Active Directory Mandanten.
Kennung	Eindeutige Kennung der dynamischen Verteilergruppe.
Bezeichnung	Bezeichnung der dynamischen Verteilergruppe.
Alias	Eindeutiger Alias zur weiteren Identifizierung der dynamischen Verteilergruppe.
Anzeigename	Anzeigename, wie er im Adressbuch verwendet wird.
Einfache Anzeige	Einfacher Anzeigename für Systeme, die nicht alle Zeichen des normalen Anzeigenamens interpretieren können.
Phonetischer Anzeigename	Anzeigename in phonetischer Schreibweise. Wird verwendet, wenn die Aussprache und Schreibweise des Namens nicht übereinstimmen.

Eigenschaft	Beschreibung
Proxy Adressen	Weitere E-Mail-Adressen zur dynamischen Verteilergruppe.
E-Mail-Adresse	E-Mail-Adresse der dynamischen Verteilergruppe.
Nicht in Adresslisten anzeigen	Gibt an, ob die dynamische Verteilergruppe in Adressbüchern angezeigt werden soll. Ist die Option aktiviert, wird die dynamische Verteilergruppe nicht in Adressbüchern angezeigt. Diese Option gilt für die Anzeige in allen Adressbüchern.
Empfängercontainer	Basiscontainer der Empfänger. Die Bedingung zur Ermittlung der Mitglieder der Verteilergruppen wird auf den gewählten Empfängercontainer und seine untergeordneten Container angewendet.
Typ des Empfängerfilters	Typ des Filters für die Empfänger.
Enthaltene Empfänger	Musterfilter, der auf dem Empfängertyp basiert. Zulässige Werte sind **AllRecipient**, **Resources**, **MailUsers**, **MailboxUsers**, **MailContacts** und **MailGroups**. Mehrere Empfängertypen können in einer kommagetrennten Liste kombiniert werden.
Empfängerfilter	Bedingung mit zusätzlichen Filterkriterien, anhand derer die Mitglieder der dynamischen Verteilergruppe bestimmt werden.
Filterregel	Filterregeln zur Bestimmung der Mitglieder in der dynamischen Verteilergruppe.
Administrator	Administrator für die dynamische Verteilergruppe. ***Um einen Administrator festzulegen*** 1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. 2. Wählen Sie unter **Tabelle** die Tabelle, welche die Kontomanager abbildet. 3. Wählen Sie unter **Administrator** den Verantwortlichen. 4. Klicken Sie **OK**.
Notizen	Weitere Informationen zur dynamischen Verteilergruppe.
Bericht an Absender	Gibt an, ob Zustellberichte an den Absender einer Nachricht gesendet werden sollen.
Bericht an Eigentümer	Gibt an, ob Zustellberichte an den Besitzer einer Nachricht gesendet werden sollen.
Moderation aktiviert	Gibt an, ob der E-Mail Benutzer moderiert wird. Legen Sie die Moderatoren über die Aufgabe **Moderatoren zuweisen** fest.

Eigenschaft	Beschreibung
	Anschließend aktivieren Sie die Option.
Senden der Benachrichtigung	Angabe, wie Absender benachrichtigt werden, wenn Sie ein Nachricht an eine moderierte dynamische Verteilergruppe senden. Zulässige Werte sind: • **Keine Benachrichtigung**: Es erfolgt keine Benachrichtigung der Absender. • **Nur Absender der eigenen Organisation benachrichtigen**: Nur interne Absender erhalten eine Benachrichtigung. • **Alle Absender benachrichtigen**: Interne und externe Absender erhalten eine Benachrichtigung.
Abwesenheitsnotiz an Absender	Gibt an, ob die Absender von Nachrichten Abwesenheitsnachrichten erhalten sollen.
Nur Nachrichten authentifizierter Benutzer einschränken	Gibt an, ob die Authentifizierungsinformationen von Absendern angefordert werden.

Verwandte Themen

- Moderatoren für Exchange Online dynamische Verteilergruppen festlegen auf Seite 199

Empfangsbeschränkungen für Exchange Online dynamische Verteilergruppen anpassen

HINWEIS: Die Zuweisungen **Postannahme erlauben** und **Postannahme verweigern** schließen einander aus. Sie können entweder festlegen, ob die Nachrichten eines Empfängers akzeptiert werden oder abgelehnt werden.

Um die Postannahme für dynamische Verteilergruppen anzupassen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten > <Azure Active Directory Mandant> > Exchange Online Administration > Empfängerkonfiguration > Dynamische Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Verteilergruppe.
3. Wählen Sie die Aufgabe **Postannahme erlauben**, um festzulegen, von welchen Empfängern Nachrichten akzeptiert werden.

- ODER -

Wählen Sie die Aufgabe **Postannahme verweigern**, um festzulegen, von welchen Empfängern Nachrichten abgelehnt werden.

4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Empfänger enthält. Zur Auswahl stehen:
    - E-Mail-aktivierte Verteilergruppen
    - Dynamische Verteilergruppen
    - Postfächer
    - E-Mail Benutzer
    - E-Mail Kontakte
    - Office 365 Gruppen
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Empfänger zu.

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

    Um eine Zuweisung zu entfernen

    - Wählen Sie den Empfänger und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Sendeberechtigungen für Exchange Online dynamische Verteilergruppen anpassen

Über die Sendeberechtigung **Senden im Auftrag von** legen Sie fest, welche Benutzer Benachrichtigungen im Auftrag der Verteilergruppe senden können.

Um die Sendeberechtigung für dynamische Verteilergruppen anzupassen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten > <Azure Active Directory Mandant> > Exchange Online Administration > Empfängerkonfiguration > Dynamische Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Verteilergruppe.
3. Wählen Sie die Aufgabe **Sendeberechtigungen zuweisen.**
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Benutzer enthält. Zur Auswahl stehen:
    - E-Mail-aktivierte Verteilergruppen
    - Postfächer

- E-Mail Benutzer

5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzer zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Benutzer und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Moderatoren für Exchange Online dynamische Verteilergruppen festlegen

Moderierte Verteilergruppen werden eingesetzt, um Nachrichten an eine dynamische Verteilergruppe durch einen Moderator zu genehmigen oder abzulehnen. Erst nach Genehmigung durch den Moderator wird die Nachricht an die Mitglieder der dynamischen Verteilergruppe weitergeleitet.

Um Moderatoren für eine dynamische Verteilergruppe festzulegen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Dynamische Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Verteilergruppe.
3. Wählen Sie die Aufgabe **Moderatoren zuweisen**.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste die Tabelle, welche die Benutzer enthält. Zur Auswahl stehen:
   - Postfächer
   - E-Mail Kontakte
   - E-Mail Benutzer
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Moderatoren zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Moderator und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Exchange Online E-Mail-aktivierte Verteilergruppen in Exchange Online dynamische Verteilergruppen aufnehmen

Um eine dynamische Verteilergruppe in E-Mail-aktivierte Verteilergruppen aufzunehmen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten > <Azure Active Directory Mandant> > Exchange Online Administration > Empfängerkonfiguration > Dynamische Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Verteilergruppe.
3. Wählen Sie die Aufgabe **E-Mail-aktivierte Verteilergruppen zuweisen** aus.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die E-Mail-aktivierten Verteilergruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von E-Mail-aktivierten Verteilergruppen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die E-Mail-aktivierte Verteilergruppe und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online dynamische Verteilergruppen in Exchange Online E-Mail-aktivierte Verteilergruppen aufnehmen auf Seite 168

Exchange Online dynamische Verteilergruppen löschen

Die dynamische Verteilergruppe wird endgültig aus der One Identity Manager-Datenbank und der Exchange Online-Umgebung gelöscht.

Um eine dynamische Verteilergruppe zu löschen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten > <Azure Active Directory Mandant> > Exchange Online Administration > Empfängerkonfiguration > Dynamische Verteilergruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Verteilergruppe.

3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Exchange Online E-Mail-aktivierte öffentliche Ordner

Öffentliche Ordner werden eingesetzt, um den Identitäten den gemeinsamen Zugriff auf Informationen zu ermöglichen. Öffentliche Ordner können hierarchisch aufgebaut sein und sind mit einer Datenbank für öffentliche Ordner verbunden. Durch die E-Mail-Aktivierung eines öffentlichen Ordners können Benutzer E-Mail Benachrichtigungen an den öffentlichen Ordner senden.

E-Mail-aktivierte öffentliche Ordner werden durch die Synchronisation in den One Identity Manager eingelesen und können im One Identity Manager nicht bearbeitet werden.

Detaillierte Informationen zum Thema

- Informationen über Exchange Online E-Mail-aktivierte öffentliche Ordner anzeigen auf Seite 202
- Exchange Online E-Mail-aktivierte Verteilergruppen an Exchange Online E-Mail-aktivierte öffentliche Ordner zuweisen auf Seite 203
- Exchange Online Öffentliche Ordner auf Seite 96
- Einzelobjekte synchronisieren auf Seite 53

Informationen über Exchange Online E-Mail-aktivierte öffentliche Ordner anzeigen

Um die Informationen zu einem E-Mail-aktivierten öffentlichen Ordner anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten > <Azure Active Directory Mandant> > Exchange Online Administration >**

Empfängerkonfiguration > E-Mail-aktivierte öffentliche Ordner.

2. Wählen Sie in der Ergebnisliste den E-Mail-aktivierten öffentlichen Ordner.
3. Wählen Sie eine der folgenden Aufgaben:
   - **Überblick über den Exchange Online E-Mail-aktivierten öffentlichen Ordner**: Sie erhalten einen Überblick über den E-Mail-aktivierten öffentlichen Ordner und seine Abhängigkeiten.
   - **Stammdaten bearbeiten**: Es werden die Stammdaten für den E-Mail-aktivierten öffentlichen Ordner angezeigt.
   - **Postannahme erlauben**: Es wird angezeigt, von welchen Empfängern Nachrichten akzeptiert werden.
   - **Postannahme verweigern**: Es wird angezeigt, von welchen Empfängern Nachrichten abgelehnt werden.
   - **Sendeberechtigung zuweisen**: Es wird angezeigt, wer im Auftrag des E-Mail-aktivierten öffentlichen Orders Nachrichten versenden kann
   - **Moderatoren zuweisen**: Es wird angezeigt, wer Nachrichten an einen moderierten E-Mail-aktivierter öffentlichen Ordner genehmigen oder ablehnen darf.
   - **E-Mail-aktivierte Verteilergruppen zuweisen**: Es wird angezeigt, welche E-Mail-aktivierten Verteilergruppen zugewiesen sind. Sie können weitere E-Mail-aktivierten Verteilergruppen zuweisen oder Zuweisungen entfernen.

Verwandte Themen

- Exchange Online E-Mail-aktivierte Verteilergruppen an Exchange Online E-Mail-aktivierte öffentliche Ordner zuweisen auf Seite 203
- Exchange Online Öffentliche Ordner auf Seite 96
- Einzelobjekte synchronisieren auf Seite 53

Exchange Online E-Mail-aktivierte Verteilergruppen an Exchange Online E-Mail-aktivierte öffentliche Ordner zuweisen

Um E-Mail-aktivierte Verteilergruppen an einen E-Mail-aktivierten öffentlichen Ordner zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten > <Azure Active Directory Mandant> > Exchange Online Administration >**

Empfängerkonfiguration > E-Mail-aktivierte öffentliche Ordner.

2. Wählen Sie in der Ergebnisliste den E-Mail-aktivierten öffentlichen Ordner.
3. Wählen Sie die Aufgabe **E-Mail-aktivierte Verteilergruppen zuweisen** aus.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die E-Mail-aktivierten Verteilergruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von E-Mail-aktivierten Verteilergruppen entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die E-Mail-aktivierte Verteilergruppe und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- Exchange Online E-Mail-aktivierte öffentliche Ordner an Exchange Online E-Mail-aktivierte Verteilergruppen zuweisen auf Seite 169

13

Berichte über Exchange Online Objekte

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

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

Tabelle 22: Berichte zur Datenqualität eines Zielsystems

Bericht	Bereitgestellt für	Beschreibung
Übersicht anzeigen	Postfach E-Mail Benutzer E-Mail Kontakt	Der Bericht zeigt einen Überblick über das Benutzerkonto und die zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Herkunft)	Postfach E-Mail Benutzer E-Mail Kontakt	Der Bericht zeigt einen Überblick über das Benutzerkonto und die Herkunft der zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Historie)	Postfach E-Mail Benutzer E-Mail Kontakt	Der Bericht zeigt einen Überblick über das Benutzerkonto einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	E-Mail-aktivierte Verteilergruppe Office 365 Gruppe	Der Bericht ermittelt alle Rollen, in denen sich Identitäten befinden, welche die ausgewählte Systemberechtigung besitzen.

Bericht	Bereitgestellt für	Beschreibung
Übersicht anzeigen	E-Mail-aktivierte Verteilergruppe Office 365 Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung und ihre Zuweisungen.
Übersicht anzeigen (inklusive Herkunft)	E-Mail-aktivierte Verteilergruppe Office 365 Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung und die Herkunft der zugewiesenen Benutzerkonten.
Übersicht anzeigen (inklusive Historie)	E-Mail-aktivierte Verteilergruppe Office 365 Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.

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 23: 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. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
TargetSystem | AzureAD | ExchangeOnline | Accounts	Erlaubt die Konfiguration der Angaben zu Empfängern.
TargetSystem | AzureAD | ExchangeOnline | Accounts | MailTemplateDefaultValues	Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage **Identität - Erstellung neues Benutzerkonto mit Standardwerten** verwendet.

Konfigurationsparameter	Bedeutung
TargetSystem | AzureAD | ExchangeOnline | DefaultAddress	Standard-E-Mail-Adresse des Empfängers von Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem | AzureAD | ExchangeOnline | MaxFullsyncDuration	Maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.
QER | ITShop | AutoPublish | O3EDL	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der automatischen Übernahme von Exchange Online E-Mail-aktivierte Verteilergruppen in den IT Shop. Ist der Parameter aktiviert, werden alle Verteilergruppen automatisch als Produkte dem IT Shop zugewiesen. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
QER | ITShop | AutoPublish | O3EDL | ExcludeList	Auflistung aller Exchange Online E-Mail-aktivierten Verteilergruppen, für die keine automatische Zuordnung zum IT Shop erfolgen soll. Jeder Eintrag ist Bestandteil eines regulären Suchmusters und unterstützt die Notation für reguläre Ausdrücke. Beispiel: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS`
QER | ITShop | AutoPublish | O3EUnifiedGroup	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der automatischen Übernahme von Office 365 Gruppen in den IT Shop. Ist der Parameter aktiviert, werden alle Gruppen automatisch als Produkte dem IT Shop zugewiesen. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Proze-

Konfigurationsparameter	Bedeutung
	duren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
QER | ITShop | AutoPublish | O3EUnifiedGroup | ExcludeList	Auflistung aller Office 365 Gruppen, für die keine automatische Zuordnung zum IT Shop erfolgen soll. Jeder Eintrag ist Bestandteil eines regulären Suchmusters und unterstützt die Notation für reguläre Ausdrücke.

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 Projektvorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 24: Abbildung der Exchange Online Schematypen

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 Exchange Online 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 25: Zulässige Verarbeitungsmethoden für Schematypen

Typ	Lesen	Hinzufügen	Löschen	Aktualisieren
Öffentlicher Ordner (`PublicFolder`)	Ja	Nein	Nein	Nein
E-Mail-aktivierte öffentlicher Ordner (`MailPublicFolder`)	Ja	Nein	Nein	Nein
Richtlinie für Rollen-zuweisungen (`RoleAssignmentPolicy`)	Ja	Nein	Nein	Nein
Postfachrichtlinie für mobile Geräte (`MobileDeviceMailboxPolicy`)	Ja	Nein	Nein	Nein
Freigaberichtlinie (`SharingPolicy`)	Ja	Nein	Nein	Nein
Aufbewahrungsrichtlinie (`RententionPolicy`)	Ja	Nein	Nein	Nein
Outlook Web App-Postfach-richtlinie (`OWAMailboxPolicy`)	Ja	Nein	Nein	Nein
E-Mail-Benutzer (`MailUser`)	Ja	Ja	Ja	Ja

Typ	Lesen	Hinzufügen	Löschen	Aktualisieren
E-Mail-Kontakt (`MailContact`)	Ja	Ja	Ja	Ja
Postfach: Ressourcenpostfach (`Mailbox`)	Ja	Ja	Ja	Ja
Postfach: Freigegebenes Postfach (`Mailbox`)	Ja	Ja	Ja	Ja
Postfach: Benutzerpostfach (`Mailbox`)	Ja	Nein	Nein	Ja
Postfach: Kalendereinstellungen (`CalendarProcessing`)	Ja	Ja	Ja	Ja
Postfach: Statistik (`Mailboxstatistics`)	Ja	Ja	Ja	Ja
E-Mail-aktivierte Verteilergruppe (`DistributionGroup`)	Ja	Ja	Ja	Ja
Dynamische Verteilergruppe (`DynamicDistributionGroup`)	Ja	Nein	Ja	Ja
Office 365-Gruppe (`UnifiedGroup`)	Ja	Ja	Ja	Ja

Anhang D

Einstellungen des Exchange Online Konnektors

Für die Systemverbindung mit dem Exchange Online Konnektor werden die folgenden Einstellungen konfiguriert.

Tabelle 26: Einstellungen des Exchange Online Konnektors

Einstellung	Bedeutung

Benutzername	Vollqualifizierter Name (FQDN) des Benutzerkonto zur Anmeldung am Exchange Online.
	Beispiel:
	`<user>@<domain.com>`
	`sync.user@<yourorganisation>.onmicrosoft.com`
	Variable: `CP_Username`

Kennwort	Kennwort zum Benutzerkonto. Variable: `CP_Password`
Bereitstellung	Interne Bezeichnung der Cloudbereitstellung. Standardwert: **O365Default** Variable: `CP_ExchangeEnvironmentName`
Organisationsname	Azure Active Directory Name der Domäne zur Anmeldung am Azure Active Directory. Beispiel: `<yourorganization>.onmicrosoft.com` Variable: CP_Organization
Verwende lokale Serverzeit als Revision	Angabe zur Revisionsfilterung. Ist der Wert **True**, wird die lokale Serverzeit des Synchronisationsservers für die Revisionsfilterung genutzt (Standard). Damit ist es nicht erforderlich Zielsystemobjekte zur

Einstellung	Bedeutung
	Revisionsbestimmung zu laden. Ist der Wert **False**, wird das Änderungsdatum der zugrunde liegenden Azure Active Directory Objekte für die Revisionsfilterung verwendet. Variable: `CP_UseLocalServerTimeAsRevision`
Max. Zeitabweichung (lokal/remote) in Minuten	Angabe zur Revisionsfilterung. Angabe der maximalen Zeitdifferenz in Minuten zwischen dem Synchronisationsserver und dem Exchange Online Server. Standardwert sind 60 Minuten. Ist die Zeitdifferenz größer als 60 Minuten, passen Sie den Wert an. Variable: `CP_LocalServerRevisionMaxDifferenceInMinutes`
Max. gleichzeitige Verbindungen	Anzahl der Verbindungen an, die maximal gleichzeitig genutzt werden sollen. Der Wert muss zwischen **1** und **20** liegen. Standardwert: **2** Variable: `CP_ConnectionPoolSize`
Definition der Windows PowerShell Befehle	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.
Anwendungs-ID	Anwendungs-ID, die beim Registrieren der Anwendung für Exchange Online PowerShell im Azure Active Directory Mandanten erzeugt wird.
Zertifikat Finger-abdruck	Fingerabdruck des selbstsignierten Zertifikates.

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 Kunden von One Identity 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

P

R

S

V

Z