

Dell™ One Identity Manager 7.1.3




Administrationshandbuch für die Anbindung
einer Microsoft Azure® Active Directory®-
Umgebung



© 2016 Dell Inc. Alle Rechte vorbehalten.

Dieses Produkt ist durch US-amerikanische und internationale Urheberschutzgesetze und Gesetze zum Schutz geistigen Eigentums geschützt. Dell™, das Dell-Logo und Dell™ One Identity Manager, Active Roles, Dell™ One Identity Password Manager und Dell™ One Identity Cloud Access Manager sind Marken von Dell Inc. in den USA und/oder anderen Gerichtsbarkeiten. Microsoft, Outlook, Active Directory, Azure, SharePoint, SQL Server, Forefront, Internet Explorer, Visual Studio, Windows Server, Windows PowerShell, Windows Vista and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. SAP, SAP R/3, SAP NetWeaver Application Server, SAP HANA und BAPI sind Marken oder eingetragene Marken der SAP AG in Deutschland und vielen anderen Ländern. IBM, DB2, RACF, Notes, Domino and LotusScript are registered trademarks of International Business Machines Corporation. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Oracle, MySQL and Java are trademarks or registered trademarks of Oracle and/or its affiliates. UNIX is a registered trademark of The Open Group. Mono ist eine eingetragene Marke von Novell, Inc. in den USA und anderen Ländern. Apache and Apache HTTP Server are trademarks of The Apache Software Foundation. Firefox is a registered trademark of the Mozilla Foundation. Safari is a registered trademark of Apple Inc. Chrome und Google sind eingetragene Marken von Google Inc., Verwendung mit Genehmigung. CA ACF2 and CA Top Secret are trademarks or registered trademarks of CA Technologies Inc. Alle anderen in diesem Dokument erwähnten Marken und Namen können Marken der jeweiligen Rechtsinhaber sein.

Legende

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

One Identity Manager Administrationshandbuch für die Anbindung einer Microsoft Azure® Active Directory®-Umgebung

Aktualisiert: November 2017

Version: 7.1.3

Inhalt

Verwalten einer Azure® Active Directory®-Umgebung	7
Architekturüberblick	7
One Identity Manager Benutzer für die Verwaltung einer Azure® Active Directory®-Umgebung	8
Einrichten der Synchronisation mit einem Azure® Active Directory® Mandanten	11
Benutzer und Berechtigungen für die Synchronisation mit dem Azure® Active Directory®	12
Integrieren des One Identity Manager als Anwendung im Azure® Active Directory®	13
Einrichten des Synchronisationsservers	13
Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Azure® Active Directory® Mandanten	17
Synchronisationsergebnisse anzeigen	23
Anpassen einer Synchronisationskonfiguration	24
Synchronisation in den Azure® Active Directory® Mandanten konfigurieren	25
Synchronisation verschiedener Azure® Active Directory® Mandanten konfigurieren	26
Schema aktualisieren	26
Nachbehandlung ausstehender Objekte	27
Provisionierung von Mitgliedschaften konfigurieren	29
Unterstützung bei der Analyse von Synchronisationsproblemen	30
Deaktivieren der Synchronisation	31
Basisdaten für die Verwaltung einer Azure® Active Directory®-Umgebung	32
Einrichten von Kontendefinitionen	33
Erstellen einer Kontendefinition	34
Stammdaten einer Kontendefinition	34
Erstellen der Automatisierungsgrade	36
Stammdaten eines Automatisierungsgrades	38
Erstellen einer Abbildungsvorschrift für IT Betriebsdaten	39
Erfassen der IT Betriebsdaten	40
Ändern der IT Betriebsdaten	42
Zuweisen der Kontendefinition an Personen	42
Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen	43
Kontendefinition an Geschäftsrollen zuweisen	44
Kontendefinition an alle Personen zuweisen	44
Kontendefinition direkt an Personen zuweisen	45
Kontendefinition an Systemrollen zuweisen	46
Kontendefinition in den IT Shop aufnehmen	46
Zuweisen der Kontendefinition an ein Zielsystem	48

Löschen einer Kontendefinition	48
Initiales Kennwort für neue Azure® Active Directory® Benutzerkonten	50
E-Mail-Benachrichtigungen über Anmeldeinformationen	52
Zielsystemverantwortliche	53
Bearbeiten eines Servers	55
Stammdaten eines Jobservers	56
Festlegen der Serverfunktionen	58
Azure® Active Directory® Unternehmensverzeichnis	60
Azure® Active Directory® Mandant	60
Allgemeine Stammdaten eines Azure® Active Directory® Mandanten	61
Informationen zum lokalen Active Directory®	62
Festlegen der Kategorien für die Vererbung von Berechtigungen	63
Synchronisationsprojekt bearbeiten	64
Azure® Active Directory® Domänen	64
Azure® Active Directory® Benutzerkonten	66
Benutzerkonten mit Personen verbinden	66
Unterstützte Typen von Benutzerkonten	67
Erfassen der Stammdaten für Azure® Active Directory® Benutzerkonten	71
Allgemeine Stammdaten eines Azure® Active Directory® Benutzerkontos	72
Kontaktdaten eines Azure® Active Directory® Benutzerkontos	75
Organisatorische Informationen eines Azure® Active Directory® Benutzerkontos	75
Informationen zum lokalen Active Directory® Benutzerkonto	76
Zusätzliche Aufgaben für die Verwaltung von Azure® Active Directory® Benutzerkonten	77
Überblick über das Azure® Active Directory® Benutzerkonto	77
Ändern des Automatisierungsgrades an einem Azure® Active Directory® Benutzerkonto	77
Azure® Active Directory® Gruppen direkt an ein Azure® Active Directory® Benutzerkonto zuweisen	78
Azure® Active Directory® Administratorrollen direkt an ein Azure® Active Directory® Benutzerkonto zuweisen	78
Azure® Active Directory® Abonnements direkt an Azure® Active Directory® Benutzerkonten zuweisen	79
Unwirksamen Azure® Active Directory® Dienstpläne direkt an Azure® Active Directory® Benutzerkonten zuweisen	79
Zusatzeigenschaften an ein Azure® Active Directory® Benutzerkonto zuweisen	80
Automatische Zuordnung von Personen zu Azure® Active Directory® Benutzerkonten	81
Bearbeiten der Suchkriterien für die automatische Personenzuordnung	83
Deaktivieren von Azure® Active Directory® Benutzerkonten	85
Löschen und Wiederherstellen von Azure® Active Directory® Benutzerkonten	86
Azure® Active Directory® Gruppen	88
Bearbeiten der Stammdaten von Azure® Active Directory® Gruppen	89

Allgemeine Stammdaten einer Azure® Active Directory® Gruppe	89
Informationen zur lokalen Active Directory® Gruppe	90
Azure® Active Directory® Gruppe an Azure® Active Directory® Benutzerkonten zuweisen	91
Azure® Active Directory® Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen	92
Azure® Active Directory® Gruppe an Geschäftsrollen zuweisen	93
Azure® Active Directory® Benutzerkonten direkt an eine Azure® Active Directory® Gruppe zuweisen	94
Azure® Active Directory® Gruppe in Systemrollen aufnehmen	94
Azure® Active Directory® Gruppe in den IT Shop aufnehmen	95
Zusätzliche Aufgaben für die Verwaltung von Azure® Active Directory® Gruppen	96
Überblick über die Azure® Active Directory® Gruppe	97
Azure® Active Directory® Gruppen in Azure® Active Directory® Gruppen aufnehmen	97
Wirksamkeit von Gruppenmitgliedschaften	98
Vererbung von Azure® Active Directory® Gruppen anhand von Kategorien	100
Eigentümer an Azure® Active Directory® Gruppen zuweisen	102
Zusatzeigenschaften an eine Azure® Active Directory® Gruppe zuweisen	102
Löschen von Azure® Active Directory® Gruppen	103
Azure® Active Directory® Administratorrollen	104
Bearbeiten der Stammdaten einer Azure® Active Directory® Administratorrolle	104
Azure® Active Directory® Administratorrollen an Azure® Active Directory® Benutzerkonten zuweisen	105
Azure® Active Directory® Administratorrolle an Abteilungen, Kostenstellen und Standorte zuweisen	106
Azure® Active Directory® Administratorrolle an Geschäftsrollen zuweisen	107
Azure® Active Directory® Benutzerkonten direkt an eine Azure® Active Directory® Administratorrolle zuweisen	108
Azure® Active Directory® Administratorrolle in Systemrollen aufnehmen	109
Azure® Active Directory® Administratorrolle in den IT Shop aufnehmen	110
Zusätzliche Aufgaben für die Verwaltung von Azure® Active Directory® Administratorrollen	111
Überblick über die Azure® Active Directory® Administratorrolle	111
Vererbung von Azure® Active Directory® Administratorrollen anhand von Kategorien	112
Zusatzeigenschaften an eine Azure® Active Directory® Administratorrolle zuweisen	112
Azure® Active Directory® Abonnements und Dienstpläne	113
Azure® Active Directory® Abonnements	113
Bearbeiten der Stammdaten von Azure® Active Directory® Abonnements	113
Azure® Active Directory® Abonnements an Azure® Active Directory® Benutzerkonten zuweisen	115
Azure® Active Directory® Abonnement an Abteilungen, Kostenstellen und Standorte zuweisen	115
Azure® Active Directory® Abonnement an Geschäftsrollen zuweisen	117

Azure® Active Directory® Benutzerkonten direkt an ein Azure® Active Directory® Abonnement zuweisen	117
Azure® Active Directory® Abonnement in Systemrollen aufnehmen	118
Azure® Active Directory® Abonnement in den IT Shop aufnehmen	119
Zusätzliche Aufgaben für die Verwaltung von Azure® Active Directory® Abonnements	120
Überblick über Azure® Active Directory® Abonnements	121
Wirksamkeit von Abonnementzuweisungen	121
Vererbung von Azure® Active Directory® Abonnements anhand von Kategorien	122
Zusatzeigenschaften an ein Azure® Active Directory® Abonnement zuweisen	122
Unwirksame Azure® Active Directory® Dienstpläne	122
Bearbeiten der Stammdaten von unwirksamen Azure® Active Directory® Dienstplänen	123
Unwirksame Azure® Active Directory® Dienstpläne an Azure® Active Directory® Benutzerkonten zuweisen	124
Unwirksamen Azure® Active Directory® Dienstplan an Abteilungen, Kostenstellen und Standorte zuweisen	124
Unwirksamen Azure® Active Directory® Dienstplan an Geschäftsrollen zuweisen	125
Azure® Active Directory® Benutzerkonten direkt an unwirksamen Azure® Active Directory® Dienstplan zuweisen	126
Unwirksamen Azure® Active Directory® Dienstplan in Systemrollen aufnehmen	127
Unwirksamen Azure® Active Directory® Dienstplan in den IT Shop aufnehmen	128
Zusätzliche Aufgaben für die Verwaltung von unwirksamen Azure® Active Directory® Dienstplänen	129
Überblick über unwirksamen Azure® Active Directory® Dienstpläne	130
Wirksamkeit von Zuweisungen unwirksamer Dienstpläne	130
Vererbung von unwirksamen Azure® Active Directory® Dienstplänen anhand von Kategorien	130
Zusatzeigenschaften an einen unwirksamen Azure® Active Directory® Dienstplan zuweisen	131
Berichte über Azure® Active Directory® Objekte	132
Übersicht aller Zuweisungen	133
Anhang: Konfigurationsparameter für die Verwaltung einer Azure® Active Directory®-Umgebung	135
Anhang: Standardprojektvorlage für Azure® Active Directory®	138
Informationen zu Dell	139
Kontaktaufnahme zu Dell	139
Technische Supportressourcen	139
Index	140

Verwalten einer Azure® Active Directory®-Umgebung

Der One Identity Manager bietet eine vereinfachte Administration der Benutzerkonten einer Azure® Active Directory®-Umgebung. Der One Identity Manager konzentriert sich auf die Einrichtung und Bearbeitung von Benutzerkonten und die Versorgung mit den benötigten Berechtigungen. Um die Benutzer mit den benötigten Berechtigungen auszustatten, werden Abonnements, Dienstpläne, Gruppen und Administratorrollen im One Identity Manager abgebildet. Damit ist es möglich, die Identity und Access Governance Prozesse wie Attestierung, Identity Audit, Management von Benutzerkonten und Systemberechtigungen, IT Shop oder Berichtsabonnements für Azure® Active Directory® Mandanten zu nutzen.

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

Durch die Datensynchronisation werden zusätzliche Informationen zum Azure® Active Directory® Unternehmensverzeichnis, wie Mandant und verifizierten Domänen 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 nur in geringem Maße möglich.

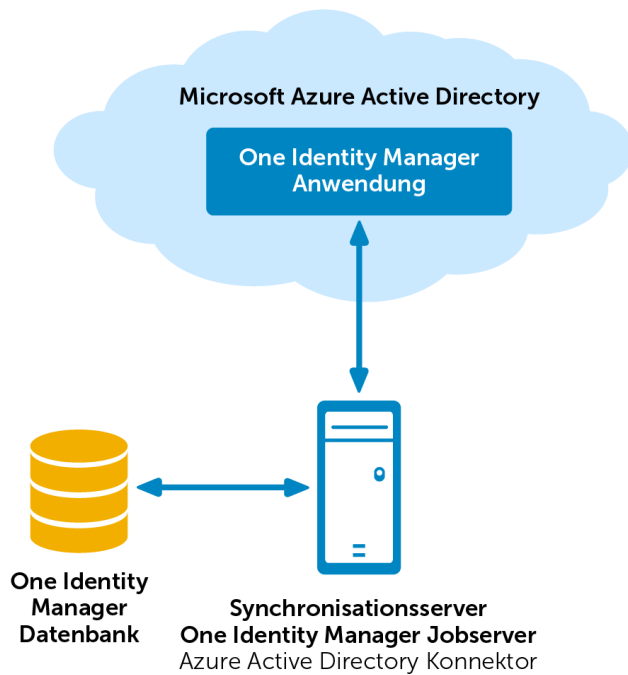
Ausführliche Informationen zur Azure® Active Directory® Struktur finden Sie in der Azure® Active Directory® Dokumentation von Microsoft.

Architekturüberblick

Um auf die Daten des Azure® Active Directory® Mandanten zuzugreifen, wird auf einem Synchronisationsserver der Azure® Active Directory® Konnektor installiert. Der Synchronisationsserver sorgt für den Abgleich der Daten zwischen der One Identity Manager-Datenbank und dem Azure® Active Directory®. Der Azure® Active Directory® Konnektor verwendet die Microsoft® Graph-API für den Zugriff auf Azure® Active Directory® Daten.

Für den Zugriff auf die Daten eines Azure® Active Directory® Mandanten, muss sich der Azure® Active Directory® Konnektor am Azure® Active Directory® Mandanten authentifizieren. Die Authentifizierung erfolgt über eine One Identity Manager Anwendung, die im Azure® Active Directory® Mandanten integriert wird und mit den entsprechenden Zugriffsberechtigungen auszustatten ist.

Abbildung 1: Architektur für die Synchronisation



One Identity Manager Benutzer für die Verwaltung einer Azure® Active Directory®-Umgebung

In die Verwaltung einer Azure® Active Directory®-Umgebung sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Zielsystemadministratoren	<p>Die Zielsystemadministratoren müssen der Anwendungsrolle Zielsysteme Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen.• Legen die Zielsystemverantwortlichen fest.• Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein.• Legen sich fest, welche Anwendungsrollen für Zielsystemverantwortliche sich widersprechen.• Berechtigen weitere Personen als Zielsystemadministratoren.• Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.
Zielsystemverantwortliche	<p>Die Zielsystemverantwortlichen müssen der Anwendungsrolle Zielsysteme Azure® Active Directory® oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Übernehmen die administrativen Aufgaben für das Zielsystem.• Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten, Gruppen oder Containerstrukturen.• Bereiten Gruppen zur Aufnahme in den IT Shop vor.• Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.• Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation.• Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Benutzer	Aufgaben
One Identity Manager Administratoren	<ul style="list-style-type: none"> • Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne.
Administratoren für den IT Shop	<p>Die Administratoren müssen der Anwendungsrolle Request & Fulfillment IT Shop Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Weisen an IT Shop-Strukturen zu.
Produkteigner für den IT Shop	<p>Die Produkteigner müssen der Anwendungsrolle Request & Fulfillment IT Shop Produkteigner oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Entscheiden über Bestellungen. • Bearbeiten die Leistungspositionen und Servicekategorien, für die sie verantwortlich sind.
Administratoren für Organisationen	<p>Die Administratoren müssen der Anwendungsrolle Identity Management Organisationen Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Weisen an Abteilungen, Kostenstellen und Standorte zu.
Administratoren für Geschäftsrollen	<p>Die Administratoren müssen der Anwendungsrolle Identity Management Geschäftsrollen Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Weisen an Geschäftsrollen zu.

Einrichten der Synchronisation mit einem Azure® Active Directory® Mandanten

Um die Objekte eines Azure® Active Directory® Mandanten 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. Integrieren Sie den One Identity Manager als Anwendung für ihren Mandanten im Azure® Active Directory® .
3. Die One Identity Manager Bestandteile für die Verwaltung von Azure® Active Directory® Mandanten sind verfügbar, wenn der Konfigurationsparameter "TargetSystem\AzureAD" aktiviert ist.
 - Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.
 - Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.
4. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
5. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Detaillierte Informationen zum Thema

- [Benutzer und Berechtigungen für die Synchronisation mit dem Azure® Active Directory® auf Seite 12](#)
- [Integrieren des One Identity Manager als Anwendung im Azure® Active Directory® auf Seite 13](#)
- [Einrichten des Synchronisationsservers auf Seite 13](#)
- [Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Azure® Active Directory® Mandanten auf Seite 17](#)
- [Deaktivieren der Synchronisation auf Seite 31](#)
- [Anpassen einer Synchronisationskonfiguration auf Seite 24](#)
- [Anhang: Konfigurationsparameter für die Verwaltung einer Azure® Active Directory®-Umgebung auf Seite 135](#)
- [Anhang: Standardprojektvorlage für Azure® Active Directory® auf Seite 138](#)

Benutzer und Berechtigungen für die Synchronisation mit dem Azure® Active Directory®

Bei der Synchronisation des One Identity Manager mit einem Azure® Active Directory® Mandanten spielen folgende Benutzer eine Rolle.

Tabelle 2: Benutzer für die Synchronisation

Benutzer	Berechtigungen
Benutzer für den Zugriff auf das Azure® Active Directory®	<p>Für eine vollständige Synchronisation von Objekten eines Azure® Active Directory® Mandanten mit der ausgelieferten One Identity Manager Standardkonfiguration stellen Sie ein Benutzerkonto bereit, das die folgenden Berechtigungen besitzt.</p> <ul style="list-style-type: none">• Mitglied in der Organisationsrolle "Globaler Administrator"
Benutzerkonto des One Identity Manager Service	<p>Das Benutzerkonto für den One Identity Manager Service benötigt die Rechte, um die Operationen auf Dateiebene durchzuführen (Rechtevergabe, Verzeichnisse und Dateien anlegen und bearbeiten).</p> <p>Das Benutzerkonto muss der Gruppe "Domänen-Benutzer" (Domain Users) angehören.</p> <p>Das Benutzerkonto benötigt das erweiterte Benutzerrecht "Anmelden als Dienst" (Log on as a service).</p> <p>Das Benutzerkonto benötigt Rechte für den internen Webservice.</p> <p>HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (NT Authority\NetworkService) laufen, so können Sie die Rechte für den internen Webservice über folgenden Kommandozeilenaufwurf vergeben:</p> <pre>netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis.</p> <p>In der Standardinstallation wird der One Identity Manager installiert unter:</p> <ul style="list-style-type: none">• %ProgramFiles(x86)%\Dell (auf 32-Bit Betriebssystemen)• %ProgramFiles%\Dell (auf 64-Bit Betriebssystemen)
Benutzer für den Zugriff auf die One Identity Manager Datenbank	<p>Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer "Synchronization" bereitgestellt.</p>

Integrieren des One Identity Manager als Anwendung im Azure® Active Directory®

Um die Daten zwischen One Identity Manager und Azure® Active Directory® zu synchronisieren, müssen Sie den One Identity Manager als Anwendung im Azure® Active Directory® Mandanten integrieren. Der Azure® Active Directory® Konnektor authentifiziert sich über die One Identity Manager Anwendung am Azure® Active Directory® Mandanten.

HINWEIS: Beim Hinzufügen des One Identity Manager als Anwendung im Azure® Active Directory® wird eine Client ID erzeugt. Diese Client ID benötigen Sie für die Einrichtung des Synchronisationsprojektes.

Ausführliche Informationen zum Integrieren von Anwendungen in Azure® Active Directory® finden Sie in der Azure® Active Directory® Dokumentation von Microsoft.

Um den One Identity Manager als Anwendung im Azure® Active Directory® zu konfigurieren

1. Melden Sie sich am Microsoft Azure Management Portal an (<https://manage.windowsazure.com>) und erstellen Sie für Ihr Verzeichnis eine neue Anwendung für den One Identity Manager.

Folgenden Einstellungen werden empfohlen:

- Wählen Sie den Link **Eine von meinem Unternehmen entwickelte Anwendung hinzufügen**.
 - Richten Sie den One Identity Manager als "systemeigene Clientanwendung" ein.
2. Konfigurieren Sie für die Anwendung folgende Einstellungen.
 - Berechtigungen für andere Anwendungen: Microsoft® Graph
 - Delegierte Berechtigungen:
 - Sign in and read user profile
 - Read and write access to user profile
 - Read and write all users' full profile
 - Read and write all groups
 - Read and write directory data
 - Access directory as the signed in user
 - Sign users in

Verwandte Themen

- [Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Azure® Active Directory® Mandanten](#) auf Seite 17

Einrichten des Synchronisationsservers

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

- Windows® Betriebssystem

Unterstützt werden die Versionen:

- Windows Server® 2008 (nicht-Itanium 64 bit) ab Service Pack 2
- Windows Server® 2008 R2 (nicht-Itanium 64 bit) ab Service Pack 1
- Windows Server® 2012
- Windows Server® 2012 R2
- Windows Server® 2016
- Microsoft® .NET Framework Version 4.5.2 oder 4.6.1
- Windows® Installer
- One Identity Manager Service, Azure® Active Directory® Konnektor
 - Installieren Sie die One Identity Manager Komponenten mit dem Installationsassistenten.
 1. Wählen Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen**.
 2. Wählen Sie die Maschinenrolle **Server | Jobserver | Azure® Active Directory®**.

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

- ① **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).
- ① **HINWEIS:** Wenn der Server, der die Synchronisation ausführt, keine direkte Verbindung zur One Identity Manager-Datenbank hat, wird die Synchronisation abgebrochen. Stellen Sie sicher, dass für diesen Server der Aufbau einer direkten Verbindung zur One Identity Manager-Datenbank möglich ist.

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

- Erstellen eines Jobservers.
- Festlegen der Maschinenrollen und Serverfunktionen für den Jobserver.
- Remote-Installation der One Identity Manager Service Komponenten entsprechend der Maschinenrollen.
- Konfigurieren des One Identity Manager Service.
- Starten des One Identity Manager Service.
- ① **HINWEIS:** Das Programm führt eine Remote-Installation des One Identity Manager Service aus. Eine lokale Installation des Dienstes ist mit diesem Programm nicht möglich. Die Remote-Installation wird nur innerhalb einer Domäne oder in Domänen mit Vertrauensstellung unterstützt.

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

1. Starten Sie das Programm Server Installer auf Ihrer administrativen Arbeitsstation.
2. Auf der Seite **Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein und klicken Sie **Weiter**.
3. Auf der Seite **Servereigenschaften** legen Sie fest, auf welchem Server der One Identity Manager Service installiert werden soll.
 - a. Wählen Sie in der Auswahlliste **Server** einen Jobserver aus.
- ODER -
Um einen neuen Jobserver zu erstellen, klicken Sie **Hinzufügen**.
 - b. Bearbeiten Sie folgende Informationen für den Jobserver.

Tabelle 3: Eigenschaften eines Jobservers

Eigenschaft	Beschreibung
Server	Bezeichnung des Jobservers.
Queue	Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Vollständiger Servername	Vollständiger Servername gemäß DNS Syntax. Beispiel: <code><Name des Servers>.<Vollqualifizierter Domänenname></code>

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

4. Auf der Seite **Maschinenrollen** legen Sie fest, welche Rolle der Jobserver im One Identity Manager übernimmt. Abhängig von der gewählten Maschinenrolle werden die Installationspakete ermittelt, die auf dem Jobserver installiert werden.
 - Azure® Active Directory®
5. Auf der Seite **Serverfunktionen** legen Sie die Funktion des Servers in der One Identity Manager-Umgebung fest. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

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

Wählen Sie mindestens folgende Serverfunktionen:

- Azure® Active Directory® Konnektor (via Microsoft® Graph)

6. Auf der Seite **Dienstkonfiguration** prüfen Sie die Konfiguration des One Identity Manager Service.
 - ① **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 Dell One Identity Manager Konfigurationshandbuch.
7. Zur Konfiguration der Remoteinstallation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** wählen Sie das Verzeichnis mit den Installationsdateien.
10. Auf der Seite **Datenbankschlüsseldatei auswählen** wählen die Datei mit dem privaten Schlüssel.
 - ① **HINWEIS:** Diese Seite wird nur angezeigt, wenn die Datenbank verschlüsselt ist.
11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.


Tabelle 4: Installationsinformationen

Eingabe	Beschreibung
Computer	<p>Server, auf dem der Dienst installiert und gestartet wird.</p> <p>Um einen Server auszuwählen</p> <ul style="list-style-type: none"> • Erfassen Sie den Servernamen. - ODER - • Wählen Sie einen Eintrag in der Liste.
Dienstkonto	<p>Angaben zum Benutzerkonto des One Identity Manager Service.</p> <p>Um ein Benutzerkonto für den One Identity Manager Service zu erfassen</p> <ul style="list-style-type: none"> • Aktivieren Sie die Option Lokales Systemkonto. Damit wird der One Identity Manager Service unter dem Konto „NT AUTHORITY\SYSTEM“ gestartet. - ODER - • Erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung.
Installationskonto	<p>Angaben zum administrativen Benutzerkonto für die Installation des Dienstes.</p> <p>Um ein administratives Benutzerkonto für die Installation zu erfassen</p> <ul style="list-style-type: none"> • Aktivieren Sie die Option Erweitert. • Aktivieren Sie die Option Angemeldeter Benutzer. Es wird das Benutzerkonto des aktuell angemeldeten Benutzers verwendet. - ODER - • Geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.

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

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

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

 **HINWEIS:** Der One Identity Manager Service wird mit der Bezeichnung „Dell One Identity Manager Service“ in der Dienstverwaltung des Servers eingetragen.


Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Azure® Active Directory® Mandanten

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

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

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

Tabelle 5: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Client ID	Client ID, die beim Hinzufügen des One Identity Manager als Anwendung des Mandanten erzeugt wird.
Anmeldedomäne	Name der Domäne zur Anmeldung am Azure® Active Directory®. Sie können die Basisdomäne oder eine verifizierte Domäne Ihres Mandanten verwenden.
Benutzerkonto und Kennwort zur Anmeldung	Benutzerkonto und Kennwort zur Authentifizierung am Azure® Active Directory® über die One Identity Manager Anwendung. Stellen Sie ein Benutzerkonto mit ausreichenden Berechtigungen bereit. Weitere Informationen finden Sie unter Benutzer und Berechtigungen für die Synchronisation mit dem Azure® Active Directory® auf Seite 12.
Schlüssel für Authentifizierung als Webanwendung	Haben Sie den One Identity Manager als Webanwendung in Ihrem Mandanten registriert, benötigen Sie den erzeugten Schlüssel.  HINWEIS: Der Schlüssel ist nur begrenzte Zeit gültig und muss nach Ablauf ausgetauscht werden.

Angaben

Erläuterungen

Synchronisationsserver für das Azure® Active Directory®

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 Azure® Active Directory® Konnektor installiert sein.

Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften.

Tabelle 6: Zusätzliche Eigenschaften für den Jobserver

Eigenschaft	Wert
Serverfunktion	Azure® Active Directory® Konnektor (via Microsoft® Graph)
Maschinenrolle	Server/Jobserver/Azure® Active Directory®

Weitere Informationen finden Sie unter [Einrichten des Synchronisationservers](#) auf Seite 13.

Verbindungsdaten zur One Identity Manager Datenbank

SQL Server®:

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

Oracle:

- Angabe, ob der Zugriff direkt oder über Oracle Client erfolgt
Die erforderlichen Verbindungsdaten sind abhängig von der Einstellung dieser Option.
- Datenbankserver
- Port der Oracle Instanz
- Service Name
- Oracle Datenbankbenutzer und Kennwort
- Datenquelle (TNS Alias Name aus der `TNSNames.ora`)

Angaben

Erläuterungen

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

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

Konfiguration des Remoteverbindungservers:

- One Identity Manager Service ist gestartet
- RemoteConnectPlugin ist installiert
- Azure® Active Directory® 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) wie der Synchronisationsserver. Nutzen Sie den Synchronisationsserver gleichzeitig als Remoteverbindungsserver, indem Sie lediglich das RemoteConnectPlugin zusätzlich installieren.

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

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

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

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

Um ein initiales Synchronisationsprojekt für einen Azure® Active Directory® Mandanten einzurichten

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
 - HINWEIS:** Wenn die Synchronisation über einen Anwendungsserver ausgeführt werden soll, stellen Sie die Datenbankverbindung über den Anwendungsserver her.
2. Wählen Sie den Eintrag **Zielsystemtyp Azure® Active Directory®**. Klicken Sie **Starten**.
Der Projektassistent des Synchronization Editors wird gestartet.
3. Auf der Seite **Systemzugriff** legen Sie fest, wie der One Identity Manager auf das Zielsystem zugreifen kann.

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

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

4. Auf der Seite **Azure® Active Directory® Mandant** geben Sie die Basisinformationen zu Ihrem Mandanten an.
 - Erfassen Sie unter **Client ID**, die Client ID, die der Integration des One Identity Manager als Anwendung des Mandanten erzeugt wurde.
 - Erfassen Sie unter **Anmeldedomäne**, die Basisdomäne oder eine verifizierte Domäne Ihres Mandanten.
5. Auf der Seite **Authentifizierung** wählen Sie die Art der Anmeldung und erfassen die benötigten Anmeldeinformationen.
 - a. Wenn Sie den One Identity Manager als systemeigene Clientanwendung in Ihrem Mandanten integriert haben, wählen Sie die Option **Authentifizierung als native Clientanwendung** und erfassen Sie das Benutzerkonto und das Kennwort zur Anmeldung am Zielsystem.
 - b. Wenn Sie den One Identity Manager als Webanwendung in Ihrem Mandanten integriert haben, wählen Sie die Option **Authentifizierung als Webanwendung** und erfassen Sie den Schlüssel, der bei der Registrierung des One Identity Manager als Anwendung des Mandanten erzeugt wurde.
6. Auf der Seite **One Identity Manager Verbindung** überprüfen Sie die Verbindungsdaten zur One Identity Manager-Datenbank. Die Daten werden aus der verbundenen Datenbank geladen. Geben Sie das Kennwort erneut ein.


① **HINWEIS:** Wenn Sie mit einer unverschlüsselten One Identity Manager-Datenbank arbeiten und noch kein Synchronisationsprojekt in der Datenbank gespeichert ist, erfassen Sie alle Verbindungsdaten neu. Wenn bereits ein Synchronisationsprojekt gespeichert ist, wird diese Seite nicht angezeigt.
7. Der Assistent lädt das Zielsystemschemata. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.
8. Auf der Seite **Zielsystemzugriff einschränken** legen Sie fest, wie der Systemzugriff erfolgen soll. Zur Auswahl stehen:

Tabelle 7: Zielsystemzugriff festlegen


Option	Bedeutung
Das Zielsystem soll nur eingelesen werden.	<p>Angabe, ob nur ein Synchronisationsworkflow zum initialen Einlesen des Zielsystems in die One Identity Manager Datenbank eingerichtet werden soll.</p> <p>Der Synchronisationsworkflow zeigt folgende Besonderheiten:</p> <ul style="list-style-type: none">• Die Synchronisationsrichtung ist "In den One Identity Manager".• In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung "In den One Identity Manager" definiert.
Es sollen auch Änderungen im Zielsystem durchgeführt werden.	<p>Angabe, ob zusätzlich zum Synchronisationsworkflow zum initialen Einlesen des Zielsystems ein Provisionierungsworkflow eingerichtet werden soll.</p> <p>Der Provisionierungsworkflow zeigt folgende Besonderheiten:</p> <ul style="list-style-type: none">• Die Synchronisationsrichtung ist "In das Zielsystem".• In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung "In das Zielsystem" definiert.• Synchronisationsschritte werden nur für solche Schemaklassen erstellt, deren Schematypen schreibbar sind.

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

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

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


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

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

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

Es wird ein Standardzeitplan für regelmäßige Synchronisationen erstellt und zugeordnet.

Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

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

- ① **HINWEIS:** Die Verbindungsdaten zum Zielsystem werden in einem Variablenset gespeichert und können bei Bedarf im Synchronization Editor in der Kategorie **Konfiguration | Variablen** angepasst werden.

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

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

- ① **HINWEIS:** Einige Inhalte erzeugen besonders viele Protokolldaten!
Das Synchronisationsprotokoll soll nur die für Fehleranalysen und weitere Auswertungen notwendigen Daten enthalten.

6. Klicken Sie **OK**.

Um regelmäßige Synchronisationen auszuführen

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

Um die initiale Synchronisation manuell zu starten

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

- HINWEIS:** Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Personen erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für den Mandanten bekannt, werden die Benutzerkonten mit den Personen verbunden. Es wird jedoch noch keine Kontendefinition zugewiesen. Die Benutzerkonten sind somit im Zustand "Linked" (verbunden).

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie dem Mandanten eine Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand "Linked" (verbunden) die Kontendefinition und den Automatisierungsgrad zu.
 - a. Wählen Sie die Kategorie **Azure® Active Directory® | Benutzerkonten | Verbunden aber nicht konfiguriert | <Mandant>**.
 - b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.

Detaillierte Informationen zum Thema

- Weitere Informationen finden Sie im Dell One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation.


Verwandte Themen

- [Integrieren des One Identity Manager als Anwendung im Azure® Active Directory®](#) auf Seite 13
- [Einrichten des Synchronisationsservers](#) auf Seite 13
- [Benutzer und Berechtigungen für die Synchronisation mit dem Azure® Active Directory®](#) auf Seite 12
- [Synchronisationsergebnisse anzeigen](#) auf Seite 23
- [Anpassen einer Synchronisationskonfiguration](#) auf Seite 24
- [Anhang: Standardprojektvorlage für Azure® Active Directory®](#) auf Seite 138
- [Einrichten von Kontendefinitionen](#) auf Seite 33
- [Automatische Zuordnung von Personen zu Azure® Active Directory® Benutzerkonten](#) auf Seite 81

Synchronisationsergebnisse anzeigen

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

Um das Protokoll einer Synchronisation anzuzeigen


1. Wählen Sie die Kategorie **Protokolle**.
2. Klicken Sie in der Symbolleiste der Navigationsansicht .

In der Navigationsansicht werden die Protokolle aller abgeschlossenen Synchronisationsläufe angezeigt.

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

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

Um das Protokoll einer Provisionierung anzuzeigen

1. Wählen Sie die Kategorie **Protokolle**.
2. Klicken Sie in der Symbolleiste der Navigationsansicht .

In der Navigationsansicht werden die Protokolle aller abgeschlossenen Provisionierungsprozesse angezeigt.

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

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

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

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt. Im Konfigurationsparameter "DPR\Journal\LifeTime" ist der Aufbewahrungszeitraum festgelegt. Standardmäßig werden Synchronisationsprotokolle 30 Tage aufbewahrt und danach gelöscht.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

- Bearbeiten Sie im Designer den Wert des Konfigurationsparameters "DPR\Journal\LifeTime". Geben Sie den Aufbewahrungszeitraum in Tagen an.

Anpassen einer Synchronisationskonfiguration

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation eines Azure® Active Directory® Mandanten eingerichtet. Mit diesem Synchronisationsprojekt können Sie Azure® Active Directory® Objekte in die One Identity Manager-Datenbank einlesen. Wenn Sie Benutzerkonten und ihre Berechtigungen mit dem One Identity Manager verwalten, werden Änderungen in die Azure® Active Directory®-Umgebung provisioniert.

Um die Datenbank und die Azure® Active Directory®-Umgebung regelmäßig abzugleichen und Änderungen zu synchronisieren, passen Sie die Synchronisationskonfiguration an.

- Um bei der Synchronisation den One Identity Manager als Mastersystem zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung "In das Zielsystem".
- Um 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.
- Mit Hilfe von Variablen kann ein Synchronisationsprojekt für die Synchronisation verschiedener Domänen eingerichtet werden. Hinterlegen Sie die Verbindungsparameter zur Anmeldung an den Domänen als Variablen.
- Um festzulegen, welche Azure® Active Directory® Objekte und Datenbankobjekte bei der Synchronisation behandelt werden, bearbeiten Sie den Scope der Zielsystemverbindung und der One

Identity Manager-Datenbankverbindung. Um Dateninkonsistenzen zu vermeiden, definieren Sie in beiden Systemen den gleichen Scope. Ist kein Scope definiert, werden alle Objekte synchronisiert.

- Wenn sich das One Identity Manager Schema oder das Zielsystemschemata geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.

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

- Wenn eine weitere Synchronisation mit derselben Startkonfiguration gestartet wird, wird dieser Prozess gestoppt und erhält den Ausführungsstatus "Froze". Es wird eine Fehlermeldung in die Protokolldatei des One Identity Manager Service geschrieben.
- Wenn eine weitere Synchronisation mit einer anderen Startkonfiguration gestartet wird, die dasselbe Zielsystem anspricht, kann das zu Synchronisationsfehlern oder Datenverlust führen. Planen Sie die Startzeiten sorgfältig. Wenn möglich, legen Sie die Startzeiten so fest, dass sich die Synchronisationen zeitlich nicht überschneiden.

Detaillierte Informationen zum Thema

- [Synchronisation in den Azure® Active Directory® Mandanten konfigurieren](#) auf Seite 25
- [Synchronisation verschiedener Azure® Active Directory® Mandanten konfigurieren](#) auf Seite 26
- [Schema aktualisieren](#) auf Seite 26
- Weitere Informationen finden Sie im Dell One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation.

Synchronisation in den Azure® Active Directory® Mandanten konfigurieren

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

Um eine Synchronisationskonfiguration für die Synchronisation in den Azure® Active Directory® Mandanten zu erstellen

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

Verwandte Themen

- [Synchronisation verschiedener Azure® Active Directory® Mandanten konfigurieren](#) auf Seite 26

Synchronisation verschiedener Azure® Active Directory® Mandanten konfigurieren

Um ein Synchronisationsprojekt für die Synchronisation eines weiteren Mandanten anzupassen

1. Stellen Sie im weiteren Mandanten ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Öffnen Sie das Synchronisationsprojekt im Synchronisation Editor.
3. Erstellen Sie für den weiteren Mandanten ein neues Basisobjekt. Verwenden Sie den Assistenten zur Anlage eines Basisobjektes.
 - Wählen Sie im Assistenten den Azure® Active Directory® Konnektor und geben Sie die Verbindungsparameter bekannt. Die Verbindungsparameter werden in einem spezialisierten Variablenset gespeichert.
Es wird eine Startkonfiguration erstellt, die das neu angelegte Variablenset verwendet.
4. Passen Sie bei Bedarf weitere Komponenten der Synchronisationskonfiguration an.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

Verwandte Themen

- [Synchronisation in den Azure® Active Directory® Mandanten konfigurieren](#) auf Seite 25

Schema aktualisieren

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

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

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

- ein Schema geändert wurde, durch:
 - Änderungen am Zielsystemschemata
 - unternehmensspezifische Anpassungen des One Identity Manager Schemas

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

Um das Schema einer Systemverbindung zu aktualisieren

1. Öffnen Sie das Synchronisationsprojekt im Synchronisation Editor.
2. Wählen Sie die Kategorie **Konfiguration | Zielsystem**.
- ODER -
Wählen Sie die Kategorie **Konfiguration | One Identity Manager Verbindung**.
3. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
Die Schemadaten werden neu geladen.

Um ein Mapping zu bearbeiten

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

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

Nachbehandlung ausstehender Objekte

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

Objekte, die als ausstehend gekennzeichnet wurden,

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

Führen Sie dafür einen Zielsystemabgleich durch.

Um ausstehende Objekte nachzubearbeiten

1. Wählen Sie die Kategorie **Azure® Active Directory® | Zielsystemabgleich: Azure® Active Directory®**.

In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp Azure® Active Directory® als Synchronisationstabellen zugewiesen sind.

- Wählen Sie in der Navigationsansicht die Tabelle, für die sie ausstehende Objekte nachbearbeiten möchten.

Das Formular für den Zielsystemabgleich wird geöffnet. Hier werden alle Objekte angezeigt, die als ausstehend markiert sind.




 **TIPP:**

Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

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

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

Tabelle 8: Methoden zur Behandlung ausstehender Objekte

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

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

- ① **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 Formularelementleiste .

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

Um kundenspezifische Tabellen in den Zielsystemabgleich aufzunehmen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Azure® Active Directory®**.
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.

- ① **HINWEIS:** Damit ausstehende Objekte in der Nachbehandlung publiziert werden können, muss der Zielsystemkonnektor schreibend auf das Zielsystem zugreifen können. Das heißt, an der Zielsystemverbindung ist die Option **Verbindung darf nur gelesen werden** deaktiviert.

Provisionierung von Mitgliedschaften konfigurieren

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

- Mitgliedschaften werden im Zielsystem in Form einer Liste als Eigenschaft eines Objekts gespeichert (Beispiel: Liste von Benutzerkonten in der Eigenschaft `Members` einer `Azure® Active Directory® Group`).
- Änderungen von Mitgliedschaften sind in beiden verbundenen Systemen zulässig.
- Ein Provisionierungsworkflow und Provisionierungsprozesse sind eingerichtet.

Wird eine Mitgliedschaft im One Identity Manager geändert, wird standardmäßig die komplette Mitgliederliste in das Zielsystem übertragen. Mitgliedschaften, die zuvor im Zielsystem hinzugefügt wurden, werden dabei entfernt; zuvor gelöschte Mitgliedschaften werden wieder eingefügt.

Um das zu verhindern, kann die Provisionierung so konfiguriert werden, dass nur die einzelne geänderte Mitgliedschaft in das Zielsystem provisioniert wird. Das entsprechende Verhalten wird für jede Zuordnungstabelle separat konfiguriert.

Um die Einzelprovisionierung von Mitgliedschaften zu ermöglichen

1. Starten Sie den Manager.
2. Wählen Sie die Kategorie **Azure® Active Directory® | Basisdaten zur Konfiguration | Zielsystemtypen**.
3. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Azure® Active Directory®**.
4. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
5. Wählen Sie die Zuordnungstabellen, für die Sie die Einzelprovisionierung ermöglichen möchten. Mehrfachauswahl ist möglich.
 - Die Option kann nur für Zuordnungstabellen aktiviert werden, deren Basistabelle eine Spalte `XDateSubItem` hat.
 - Zuordnungstabellen, die im Mapping in einer virtuellen Schemaeigenschaft zusammengefasst sind, müssen identisch markiert werden (beispielsweise `AADUserInGroup` und `AADGroupInGroup`).
6. Klicken Sie **Änderungen zusammenführen**.
7. Speichern Sie die Änderungen.

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

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

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

Unterstützung bei der Analyse von Synchronisationsproblemen

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

- Ergebnisse der Konsistenzprüfung
- Einstellungen zur Revisionsfilterung
- Verwendeter Scope

- Analyse des Synchronisationspuffers
- Zugriffszeiten auf die Objekte in der One Identity Manager Datenbank und im Zielsystem

Um den Synchronisationsanalysebericht zu erstellen

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

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

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

Deaktivieren der Synchronisation

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

Um regelmäßige Synchronisationen zu verhindern

- Wählen Sie die Startkonfiguration und deaktivieren Sie den hinterlegten Zeitplan.

Synchronisationen können nun nur noch manuell gestartet werden.

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

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

Um das geladene Synchronisationsprojekt zu deaktivieren

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

Detaillierte Informationen zum Thema

- [Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Azure® Active Directory® Mandanten](#) auf Seite 17

Basisdaten für die Verwaltung einer Azure® Active Directory®-Umgebung

Für die Verwaltung einer Azure® Active Directory®-Umgebung im One Identity Manager sind folgende Basisdaten relevant.

- Konfigurationsparameter

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

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

Weitere Informationen finden Sie unter [Anhang: Konfigurationsparameter für die Verwaltung einer Azure® Active Directory®-Umgebung](#) auf Seite 135.

- Kontendefinitionen

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

Weitere Informationen finden Sie unter [Einrichten von Kontendefinitionen](#) auf Seite 33.

- Initiales Kennwort für neue Benutzerkonten

Um das initiale Kennwort für Benutzerkonten zu vergeben, stehen Ihnen verschiedene Möglichkeiten zur Verfügung. Es kann das zentrale Kennwort der zugeordneten Person auf das Kennwort des Benutzerkontos abgebildet werden, es kann ein fest vorgegebenes Kennwort verwendet werden oder ein zufällig generiertes initiales Kennwort vergeben werden.

Weitere Informationen finden Sie unter [Initiales Kennwort für neue Azure® Active Directory® Benutzerkonten](#) auf Seite 50.

- E-Mail-Benachrichtigungen über die Anmeldeinformationen

Bei Erstellung eines neuen Benutzerkontos 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.

Weitere Informationen finden Sie unter [E-Mail-Benachrichtigungen über Anmeldeinformationen](#) auf Seite 52.

- Zielsystemtypen

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

Weitere Informationen finden Sie unter [Nachbehandlung ausstehender Objekte](#) auf Seite 27.

- Zielsystemverantwortliche

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

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

Weitere Informationen finden Sie unter [Zielsystemverantwortliche](#) auf Seite 53.

- Server

Für die Verarbeitung der Azure® Active Directory® spezifischen Prozesse im One Identity Manager müssen die Server mit ihren Serverfunktionen bekannt sein. Dazu gehört beispielsweise der Synchronisationsserver.

Weitere Informationen finden Sie unter [Bearbeiten eines Servers](#) auf Seite 55.

Einrichten von Kontendefinitionen

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

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


Ausführliche Informationen zu den Grundlagen finden Sie im Dell One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

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

Erstellen einer Kontendefinition

Um eine Kontendefinition zu erstellen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
-ODER-
Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Kontendefinition.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- [Stammdaten einer Kontendefinition](#) auf Seite 34

Stammdaten einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 9: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte Kontendefinition	Vorausgesetzte Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch mitbestellt oder zugeordnet. Für einen Azure® Active Directory® Mandanten lassen Sie die Angabe leer.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatisierungsgrad (initial)	Standardautomatisierungsgrad, der bei Neuanlage von Benutzerkonten standardmäßig verwendet werden soll.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Kontendefinition an Personen. Erfassen Sie einen Wert zwischen 0 und 1. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter "QER\CalculateRiskIndex" aktiviert ist. Weitere Informationen finden Sie im Dell 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.

Eigenschaft	Beschreibung
IT Shop	Angabe, ob die Kontendefinition über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Personen und Rollen außerhalb des IT Shop zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von den Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig.
Automatische Zuweisung zu Personen	<p>Angabe, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Beim Speichern wird die Kontendefinition an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine Person neu angelegt wird, erhält sie ebenfalls automatisch diese Kontendefinition.</p> <p>WICHTIG: Aktivieren Sie diese Option nur, wenn sichergestellt ist, dass alle aktuell in der Datenbank vorhandenen internen Personen sowie alle zukünftig neu hinzuzufügenden internen Personen ein Benutzerkonto in diesem Zielsystem erhalten sollen!</p> <p>Um die automatische Zuweisung der Kontendefinition an alle Personen zu entfernen, deaktivieren Sie die Option. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.</p>
Kontendefinition bei dauerhafter Deaktivierung beibehalten	<p>Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Personen.</p> <p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>
Kontendefinition bei zeitweiliger Deaktivierung beibehalten	<p>Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Personen.</p> <p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>
Kontendefinition bei verzögertem Löschen beibehalten	<p>Angabe zur Zuweisung der Kontendefinition bei verzögertem Löschen von Personen.</p> <p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>

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

Erstellen der Automatisierungsgrade

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

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

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

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

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

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

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


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

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

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

① | **WICHTIG:** Der Automatisierungsgrad "Unmanaged" wird beim Erstellen einer Kontendefinition automatisch zugewiesen und kann nicht entfernt werden.

Um einen Automatisierungsgrad zu bearbeiten

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

Um Kontendefinitionen an einen Automatisierungsgrad zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Basisdaten zur Konfiguration | Kontendefinitionen | Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad.
3. Wählen Sie die Aufgabe **Kontendefinitionen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontendefinitionen zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Kontendefinitionen.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- [Stammdaten eines Automatisierungsgrades](#) auf Seite 38

Stammdaten eines Automatisierungsgrades

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 10: Stammdaten eines Automatisierungsgrades

Eigenschaft	Beschreibung
Automatisierungsgrad	Bezeichnung des Automatisierungsgrades.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Betriebsdaten überschreibend	Angabe, ob Daten an Benutzerkonten, die sich aus den IT Betriebsdaten bilden, automatisch aktualisiert werden. Zulässige Werte sind: Niemals Die Daten werden nicht aktualisiert. Immer Die Daten werden immer aktualisiert Nur initial Die Daten werden nur initial ermittelt.
Gruppen bei zeitweiliger Deaktivierung beibehalten	Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei zeitweiliger Deaktivierung sperren	Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen gesperrt werden sollen.
Gruppen bei dauerhafter Deaktivierung beibehalten	Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei dauerhafter Deaktivierung sperren	Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen gesperrt werden sollen.
Gruppen bei verzögertem Löschen beibehalten	Angabe, ob die Benutzerkonten zum Löschen markierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei verzögertem Löschen sperren	Angabe, ob die Benutzerkonten zum Löschen markierter Personen gesperrt werden sollen.
Gruppen bei Sicherheitsgefährdung beibehalten	Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei Sicherheitsgefährdung sperren	Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen gesperrt werden sollen.
Gruppen bei deaktiviertem Benutzerkonto beibehalten	Angabe, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen.

Erstellen einer Abbildungsvorschrift für IT Betriebsdaten

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

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


- Gruppen erbbar
- Identität
- Privilegiertes Benutzerkonto
- Kennwort bei der nächsten Anmeldung ändern

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

1. Wählen Sie 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 Mapping bearbeiten**.

4. Erfassen Sie die folgenden Daten.

Tabelle 11: Abbildungsvorschrift für IT Betriebsdaten

Eigenschaft	Beschreibung
Spalte	Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird.
Quelle	Angabe, welche Rolle verwendet wird, um die Eigenschaften für das Benutzerkonto zu ermitteln. Zur Auswahl stehen: <ul style="list-style-type: none">• Primäre Abteilung• Primärer Standort• Primäre Kostenstelle• Primäre Geschäftsrolle <p> HINWEIS: Verwenden Sie die primäre Geschäftsrolle nur, wenn das Geschäftsrollenmodul vorhanden ist.</p> <ul style="list-style-type: none">• keine Angabe <p>Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option Immer Standardwert verwenden setzen.</p>
Standardwert	Standardwert der Eigenschaft für das Benutzerkonto einer Person, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann.
Immer Standardwert verwenden	Angabe, ob die Eigenschaft des Benutzerkontos immer mit dem Standardwert besetzt wird. Es erfolgt keine dynamische Ermittlung der IT Betriebsdaten aus einer Rolle.
Benachrichtigung bei Verwendung des Standards	Angabe, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage "Person - Erstellung neues Benutzerkontos mit Standardwerten" verwendet. Um die Mailvorlage zu ändern, passen Sie den Konfigurationsparameter "TargetSystem\AzureAD\Accounts\MailTemplateDefaultValues" an.

5. Speichern Sie die Änderungen.

Verwandte Themen

- [Erfassen der IT Betriebsdaten](#) auf Seite 40

Erfassen der IT Betriebsdaten

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

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

Beispiel:

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


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

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

Um IT Betriebsdaten festzulegen

1. Wählen Sie in der Kategorie **Organisationen** bzw. **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten**.
3. Erfassen Sie die folgenden Daten.

Tabelle 12: IT Betriebsdaten

Eigenschaft	Beschreibung
Organisation/Geschäftsrolle	Abteilung, Kostenstelle, Standort oder Geschäftsrolle, für die die IT Betriebsdaten gelten sollen.
Wirksam für	Anwendungsbereich der IT Betriebsdaten. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden.
Um den Anwendungsbereich festzulegen	
	<ol style="list-style-type: none"> a. Klicken Sie auf die Schaltfläche  neben dem Eingabefeld. b. Wählen Sie unter Tabelle die Tabelle, die das Zielsystem abbildet oder für eine Kontendefinition die Tabelle <code>TSBAccountDef</code>. c. Wählen Sie unter Wirksam für das konkrete Zielsystem oder die konkrete Kontendefinition. d. Klicken Sie OK.
Spalte	Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript <code>TSB_ITDataFromOrg</code> verwenden. Ausführliche Informationen dazu finden Sie im Dell One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.
Wert	Konkreter Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.

4. Speichern Sie die Änderungen.

Verwandte Themen

- [Erstellen einer Abbildungsvorschrift für IT Betriebsdaten](#) auf Seite 39

Ändern der IT Betriebsdaten

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

Voraussetzungen

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

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

Um die Bildungsregeln auszuführen

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

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

Alter Wert: Aktueller Wert der Objekteigenschaft.

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

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

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

Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinition an Personen

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

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

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

- ① **HINWEIS:** Ist bereits ein Benutzerkonto vorhanden und ist es deaktiviert, dann wird dieses Benutzerkonto entsperrt. Den Automatisierungsgrad des Benutzerkontos müssen Sie in diesem Fall nachträglich ändern.

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

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

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

Detaillierte Informationen zum Thema

- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 43
- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 44
- [Kontendefinition an alle Personen zuweisen](#) auf Seite 44
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 45
- [Kontendefinition an Systemrollen zuweisen](#) auf Seite 46
- [Kontendefinition in den IT Shop aufnehmen](#) auf Seite 46

Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

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

Verwandte Themen

- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 44
- [Kontendefinition an alle Personen zuweisen](#) auf Seite 44
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 45
- [Kontendefinition an Systemrollen zuweisen](#) auf Seite 46
- [Kontendefinition in den IT Shop aufnehmen](#) auf Seite 46

Kontendefinition an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

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

Verwandte Themen

- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 43
- [Kontendefinition an alle Personen zuweisen](#) auf Seite 44
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 45
- [Kontendefinition an Systemrollen zuweisen](#) auf Seite 46
- [Kontendefinition in den IT Shop aufnehmen](#) auf Seite 46

Kontendefinition an alle Personen zuweisen

Um eine Kontendefinition an alle Personen zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.

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

5. Speichern Sie die Änderungen.

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

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

Verwandte Themen

- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 43
- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 44
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 45
- [Kontendefinition an Systemrollen zuweisen](#) auf Seite 46
- [Kontendefinition in den IT Shop aufnehmen](#) auf Seite 46

Kontendefinition direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **An Personen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Personen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 43
- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 44
- [Kontendefinition an alle Personen zuweisen](#) auf Seite 44
- [Kontendefinition an Systemrollen zuweisen](#) auf Seite 46
- [Kontendefinition in den IT Shop aufnehmen](#) auf Seite 46

Kontendefinition an Systemrollen zuweisen

Installierte Module: Systemrollenmodul

- ① **HINWEIS:** Kontendefinitionen, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können Sie nur an Systemrollen zuweisen, bei denen diese Option ebenfalls aktiviert ist.

Um Kontendefinitionen in eine Systemrolle aufzunehmen

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

Verwandte Themen

- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 43
- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 44
- [Kontendefinition an alle Personen zuweisen](#) auf Seite 44
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 45
- [Kontendefinition in den IT Shop aufnehmen](#) auf Seite 46

Kontendefinition in den IT Shop aufnehmen

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

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

- ① **HINWEIS:** Bei rollenbasierter Anmeldung können die IT Shop Administratoren Kontendefinitionen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Kontendefinition in den IT Shop aufzunehmen.

Um eine Kontendefinition in den IT Shop aufnehmen

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

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

Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen

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

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).
- ODER -
Wählen Sie die Kategorie **Berechtigungen | Kontendefinitionen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

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

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

Verwandte Themen

- [Stammdaten einer Kontendefinition auf Seite 34](#)
- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 43](#)
- [Kontendefinition an Geschäftsrollen zuweisen auf Seite 44](#)
- [Kontendefinition an alle Personen zuweisen auf Seite 44](#)
- [Kontendefinition direkt an Personen zuweisen auf Seite 45](#)
- [Kontendefinition an Systemrollen zuweisen auf Seite 46](#)

Zuweisen der Kontendefinition an ein Zielsystem

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

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

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

Um die Kontendefinition an ein Zielsystem zuzuweisen

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

Detaillierte Informationen zum Thema

- [Automatische Zuordnung von Personen zu Azure® Active Directory® Benutzerkonten](#) auf Seite 81

Löschen einer Kontendefinition


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

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

Um eine Kontendefinition zu löschen

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Personen.
 - a. Wählen Sie die Kategorie **Azure® Active Directory® | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
 - b. Wählen Sie in der Ergebnisliste die Kontendefinition.
 - c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
 - d. Deaktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.
 - e. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Personen.
 - a. Wählen Sie die Kategorie **Azure® Active Directory® | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
 - b. Wählen Sie in der Ergebnisliste die Kontendefinition.

- c. Wählen Sie die Aufgabe **An Personen zuweisen**.
 - d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Personen.
 - e. Speichern Sie die Änderungen.
3. Entfernen Sie die Zuordnung der Kontendefinition zu Abteilungen, Kostenstellen und Standorte.
- a. Wählen Sie 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 die Kategorie **Azure® Active Directory® | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
 - b. Wählen Sie in der Ergebnisliste die Kontendefinition.
 - c. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
 - d. Speichern Sie die Änderungen.
5. Wenn die Kontendefinition über den IT Shop bestellt wurde, muss sie abbestellt und aus allen IT Shop Regalen entfernt werden. Ausführliche Informationen dazu finden Sie im Dell One Identity Manager Administrationshandbuch für IT Shop.
6. Entfernen Sie die Zuordnung der Kontendefinition als vorausgesetzte Kontendefinition einer anderen Kontendefinition. Solange die Kontendefinition Voraussetzung einer anderen Kontendefinition ist, kann sie nicht gelöscht werden. Prüfen Sie alle Kontendefinitionen.
- a. Wählen Sie die Kategorie **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 in der Kategorie **Azure® Active Directory® | Mandanten** den Mandanten.
 - b. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
 - c. Entfernen Sie auf dem Tabreiter **Allgemein** die zugewiesenen Kontendefinitionen.
 - d. Speichern Sie die Änderungen.
8. Löschen Sie die Kontendefinition.
- a. Wählen Sie 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.

Initiales Kennwort für neue Azure® Active Directory® Benutzerkonten

Tabelle 13: Konfigurationsparameter für die Bildung eines initialen Kennwortes für Benutzerkonten

Konfigurationsparameter	Bedeutung
QER\Person\CentralPasswordHistoryLength	Der Konfigurationsparameter legt fest, ob eine Kennwortchronik erstellt wird. Der angegebene Wert entspricht der Anzahl der eindeutigen neuen Kennwörter, bevor ein altes Kennwort erneut verwendet werden kann. Getestet wird das zentrale Kennwort der Person.
QER\Person\UseCentralPassword	Der Konfigurationsparameter legt fest, ob das zentrale Kennwort der Person automatisch auf die Benutzerkonten der Person in allen erlaubten Zielsystemen abgebildet wird.
QER\Person\UseCentralPassword\PermanentStore	Der Konfigurationsparameter steuert die Aufbewahrungszeit der zentralen Kennwörter. Ist der Parameter aktiviert, wird das zentrale Kennwort der Person dauerhaft gespeichert. Ist der Parameter nicht aktiviert, wird das zentrale Kennwort nur zum Publizieren in die Zielsysteme benutzt und anschließend in der One Identity Manager-Datenbank gelöscht.
TargetSystem\AzureAD\Accounts\InitialPassword	Der Konfigurationsparameter enthält das initiale Kennwort für neu erzeugte Benutzerkonten. Wird beim Anlegen im Benutzerkonto selbst kein Kennwort angegeben, dann wird das initiale Kennwort aus dem Konfigurationsparameter benutzt. Dies kann erforderlich sein, wenn ein Benutzerkonto im Zielsystem angelegt werden muss und die Zielsystemumgebung eine minimale Kennwortlänge > 0 erfordert. Für das initiale Kennwort ist die minimale Kennwortlänge zu beachten.
TargetSystem\AzureAD\Accounts\InitialRandomPassword	Der Konfigurationsparameter legt fest, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in den Konfigurationsparametern unterhalb gesetzt sind.

Konfigurationsparameter	Bedeutung
TargetSystem\AzureAD\Accounts\InitialRandomPassword\Character	Der Konfigurationsparameter legt fest, ob das Zufallskennwort mindestens einen Buchstaben [a-z] enthalten muss.
TargetSystem\AzureAD\Accounts\InitialRandomPassword\Length	Der Konfigurationsparameter legt fest, wie viele Zeichen das Zufallskennwort enthalten muss.
TargetSystem\AzureAD\Accounts\InitialRandomPassword\numeric	Der Konfigurationsparameter legt fest, ob im Zufallskennwort mindestens eine Ziffer [0-9] enthalten sein muss.
TargetSystem\AzureAD\Accounts\InitialRandomPassword\SpecialCharacter	Der Konfigurationsparameter legt fest, ob im Zufallskennwort mindestens ein Sonderzeichen enthalten sein muss.
TargetSystem\AzureAD\Accounts\InitialRandomPassword\UpperCase	Der Konfigurationsparameter legt fest, ob im Zufallskennwort mindestens einen Großbuchstaben [A-Z] enthalten sein muss.

Um das initiale Kennwort für neue Azure® Active Directory® Benutzerkonten zu vergeben, stehen Ihnen verschiedene Möglichkeiten zur Verfügung.

1. Das zentrale Kennwort der zugeordneten Person wird auf das Kennwort des Benutzerkontos abgebildet.
 - Aktivieren Sie im Designer den Konfigurationsparameter "QER\Person\UseCentralPassword".
Ist der Konfigurationsparameter „QER\Person\UseCentralPassword“ aktiviert, wird das zentrale Kennwort der Person automatisch auf die Benutzerkonten einer Person in den einzelnen Zielsystemen abgebildet.
 - Aktivieren Sie im Designer den Konfigurationsparameter „QER\Person\UseCentralPassword\PermanentStore“ und legen Sie fest, ob das zentrale Kennwort der Personen dauerhaft oder nur bis zum Publizieren in die Zielsysteme in der One Identity Manager-Datenbank gespeichert wird.
 - Aktivieren Sie im Designer den Konfigurationsparameter „QER\Person\CentralPasswordHistoryLength“. Der Konfigurationsparameter steuert die Kennwortchronik. Der angegebene Wert entspricht der Anzahl der eindeutigen neuen Kennwörter, bevor ein altes Kennwort erneut verwendet werden kann. Getestet wird das zentrale Kennwort der Person.
2. Ein fest vorgegebenes Kennwort wird automatisch bei Erstellen eines Benutzerkontos eingetragen.
 - Aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\AzureAD\Accounts\InitialPassword" und tragen Sie als Wert das initiale Kennwort ein.
 - ① **HINWEIS:** Um das Kennwort zu verschlüsseln, setzen Sie die Option **Verschlüsselt** am Konfigurationsparameter.
3. Bei der Neuanlage eines Benutzerkontos wird ein zufällig generiertes initiales Kennwort vergeben.
 - Aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\AzureAD\Accounts\InitialRandomPassword" und seine untergeordneten Konfigurationsparameter.

Über die untergeordneten Konfigurationsparameter bestimmen Sie die Zeichenklassen, die dieses Kennwort enthalten muss und legen fest, an welche Person das initiale Kennwort per E-Mail versendet wird.

Verwandte Themen

- [E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 52](#)

E-Mail-Benachrichtigungen über Anmeldeinformationen

Tabelle 14: Konfigurationsparameter für Benachrichtigungen über Anmeldeinformationen

Konfigurationsparameter	Bedeutung
TargetSystem\ AzureAD \Accounts\InitialRandomPassword	Der Konfigurationsparameter legt fest, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in den Konfigurationsparametern unterhalb gesetzt sind.
TargetSystem\AzureAD \Accounts\InitialRandomPassword\SendTo	Der Konfigurationsparameter enthält die Person, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle /Abteilung/Standort/Geschäftsrolle, Verantwortlicher der Person oder XUserInserted). Ist kein Empfänger ermittelbar, dann wird an die im Konfigurationsparameter "TargetSystem\AzureAD\DefaultAddress" hinterlegte Adresse versandt.
TargetSystem\AzureAD\Accounts\ InitialRandomPassword\SendTo\ MailTemplateAccountName	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den initialen Anmeldeinformationen (Name des Benutzerkontos) zu versorgen.
TargetSystem\AzureAD\Accounts\ InitialRandomPassword\SendTo\ MailTemplatePassword	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den initialen Anmeldeinformationen (initiales Kennwort) zu versorgen.
TargetSystem\AzureAD\DefaultAddress	Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem.

Die Anmeldeinformationen für neue Benutzerkonten können per E-Mail an eine festgelegte Person gesendet werden. Dabei werden zwei Benachrichtigungen versendet, die den Benutzernamen und das initiale Kennwort enthalten. Zur Erzeugung der Benachrichtigungen werden Mailvorlagen genutzt. In einer Mailvorlage sind die Mailtexte in verschiedenen Sprachen definiert. Somit wird bei Generierung einer E-Mail Benachrichtigung die Sprache des Empfängers berücksichtigt. In der Standardinstallation sind bereits Mailvorlagen enthalten, die Sie zur Konfiguration der Benachrichtigungsverfahren verwenden können.

Um Benachrichtigungen über Anmeldeinformationen zu nutzen

1. Stellen Sie sicher, dass das E-Mail-Benachrichtungssystem im One Identity Manager konfiguriert ist. Ausführliche Informationen finden Sie im Dell One Identity Manager Konfigurationshandbuch.
2. Aktivieren Sie im Designer den Konfigurationsparameter „Common\MailNotification\DefaultSender“ und geben Sie die Absenderadresse an, mit der die E-Mail Benachrichtigungen verschickt werden.
3. Stellen Sie sicher, dass alle Personen eine Standard-E-Mail-Adresse besitzen. An diese E-Mail Adresse werden die Benachrichtigungen versendet. Ausführliche Informationen finden Sie im Dell One Identity Manager Administrationshandbuch für das Identity Management Basismodul.
4. Stellen Sie sicher, dass für alle Personen eine Sprachkultur ermittelt werden kann. Nur so erhalten die Personen die E-Mail Benachrichtigungen in ihrer Sprache. Ausführliche Informationen finden Sie im Dell One Identity Manager Administrationshandbuch für das Identity Management Basismodul.

Wenn bei der Neuanlage eines Benutzerkontos ein zufällig generiertes initiales Kennwort vergeben wird, werden die initialen Anmeldeinformationen für dieses Benutzerkonto per E-Mail an eine vorher festgelegt Person gesendet.

Um die initialen Anmeldeinformationen per E-Mail zu versenden

1. Aktivieren Sie im Designer den Konfigurationsparameter „TargetSystem\AzureAD\Accounts\InitialRandomPassword“.
2. Aktivieren Sie im Designer den Konfigurationsparameter „TargetSystem\AzureAD\Accounts\InitialRandomPassword\SendTo“ und erfassen Sie als Wert den Empfänger der Benachrichtigung.
3. Aktivieren Sie im Designer den Konfigurationsparameter „TargetSystem\AzureAD\Accounts\InitialRandomPassword\SendToMailTemplateAccountName“.

Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage „Person - Erstellung neues Benutzerkonto“ versendet. Die Benachrichtigung enthält den Namen des Benutzerkontos.

4. Aktivieren Sie im Designer den Konfigurationsparameter „TargetSystem\AzureAD\Accounts\InitialRandomPassword\SendToMailTemplatePassword“.
- Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage „Person - Initiales Kennwort für neues Benutzerkonto“ versendet. Die Benachrichtigung enthält das initiale Kennwort für das Benutzerkonto.

TIPP: Um andere als die Standardmailvorlagen für diese Benachrichtigungen zu nutzen, ändern Sie den Wert der Konfigurationsparameter.

Zielsystemverantwortliche

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

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

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

Zielsystemverantwortliche der Standardanwendungsrolle sind berechtigt alle Mandanten im One Identity Manager zu bearbeiten.

3. Zielsystemverantwortliche können innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche berechtigen und bei Bedarf weitere untergeordnete Anwendungsrollen erstellen und einzelnen Mandanten zuweisen.

Tabelle 15: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	<p>Die Zielsystemverantwortlichen müssen der Anwendungsrolle Zielsysteme Azure® Active Directory® oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Übernehmen die administrativen Aufgaben für das Zielsystem.• Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten, Gruppen oder Containerstrukturen.• Bereiten Gruppen zur Aufnahme in den IT Shop vor.• Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.• Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation.• Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Um initial Personen als Zielsystemadministrator festzulegen

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

Um initial Personen in die Standardanwendungsrolle für Zielsystemverantwortliche aufzunehmen

1. Melden Sie sich als Zielsystemadministrator (Anwendungsrolle **Zielsysteme | Administratoren**) am Manager an.
2. Wählen Sie die Kategorie **One Identity Manager Administration | Zielsysteme | Azure® Active Directory®**.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Personen zu und speichern Sie die Änderungen.


Um als Zielsystemverantwortlicher weitere Personen als Zielsystemverantwortliche zu berechtigen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie in der Kategorie **Azure® Active Directory® | Basisdaten zur Konfiguration | Zielsystemverantwortliche** die Anwendungsrolle.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Personen zu und speichern Sie die Änderungen.

Um Zielsystemverantwortliche für einzelne Mandanten festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **Azure® Active Directory® | Mandanten**.
3. Wählen Sie in der Ergebnisliste den Mandanten.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Zielsystemverantwortliche** die Anwendungsrolle.

- ODER -

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

- Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Zielsysteme | Azure® Active Directory®** zu.
 - Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.
6. Speichern Sie die Änderungen.
 7. Weisen Sie der Anwendungsrolle die Personen zu, die berechtigt sind, den Mandanten im One Identity Manager zu bearbeiten.

Verwandte Themen

- [One Identity Manager Benutzer für die Verwaltung einer Azure® Active Directory®-Umgebung auf Seite 8](#)
- [Azure® Active Directory® Mandant auf Seite 60](#)

Bearbeiten eines Servers

Für die Verarbeitung der Azure® Active Directory® 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 einen Eintrag für den Jobserver.
- 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.

- i **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 Dell One Identity Manager Installationshandbuch beschrieben vor.

Um einen Jobserver und seine Funktionen zu bearbeiten

1. Wählen Sie 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.

- i **HINWEIS:** Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten | Jobserver** zur Verfügung.

Detaillierte Informationen zum Thema

- [Stammdaten eines Jobservers](#) auf Seite 56
- [Festlegen der Serverfunktionen](#) auf Seite 58

Stammdaten eines Jobservers

- i **HINWEIS:** Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten | Jobserver** zur Verfügung.

Tabelle 16: Eigenschaften eines Jobservers

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS Syntax. Beispiel: <code><Name des Servers>.<Vollqualifizierter Domänenname></code>
Zielsystem	Zielsystem des Computerkontos.
Sprachkultur	Sprache des Servers.
Server ist Cluster	Angabe, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. i 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.

Eigenschaft	Bedeutung
Kopierverfahren (Quellserver)	<p>Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Quelle einer Kopieraktion ist. Derzeit werden nur Kopierverfahren über die Programme „Robocopy“ und „rsync“ unterstützt.</p> <p>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.</p>
Kopierverfahren (Zielserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Ziel einer Kopieraktion ist.
Codierung	Codierung des Zeichensatzes mit der Dateien auf dem Server geschrieben werden.
Übergeordneter Jobserver	Bezeichnung des übergeordneten Jobservers.
Ausführender Server	<p>Bezeichnung des ausführenden Servers. Eingetragen wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden.</p> <p>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.</p>
Queue	Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
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	<p>Angabe, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur <code>QBM_PJobQueueLoad</code> aktiviert, sobald die Queue das erste Mal angefragt wird.</p> <p>Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.</p>

Eigenschaft	Bedeutung
Stopp One Identity Manager Service	Angabe, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten. Den Dienst können Sie mit entsprechenden administrativen Rechten im Programm "Job Queue Info" stoppen und starten.
kein automatisches Softwareupdate	Angabe, ob die von der automatischen Softwareaktualisierung auszuschließen sind. ⓘ HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.
Softwareupdate läuft	Angabe, 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 58

Festlegen der Serverfunktionen

ⓘ | **HINWEIS:** Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten** | **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 17: Zulässige Serverfunktionen

Serverfunktion	Anmerkungen
Azure® Active Directory® Konnektor (via Microsoft Graph)	Server, auf dem der Azure® Active Directory® Konnektor installiert ist. Der Server führt die Synchronisation mit dem Zielsystem Azure® Active Directory® aus.
CSV Konnektor	Server, auf dem der CSV Konnektor für die Synchronisation installiert ist.
Domänen-Controller	Active Directory® Domänen-Controller. Server, die nicht als Domänen-Controller gekennzeichnet sind, werden als Memberserver betrachtet.
Druckserver	Server, der als Druckserver arbeitet.
Generischer Server	Server für die generische Synchronisation mit einem kundendefinierten Zielsystem.
Homeserver	Server zur Anlage von Homeverzeichnissen für Benutzerkonten.
Master SQL Server	Server, der die Datenbankabfragen verarbeitet. Der Server wird bereits während der initialen Schemainstallation eingetragen.

Serverfunktion	Anmerkungen
Nativer Datenbankkonnektor	Der Server kann sich mit einer ADO.Net Datenbank verbinden.
One Identity Manager Datenbankkonnektor	Server, auf dem der One Identity Manager Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem One Identity Manager aus.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
Primärer Domänen-Controller	Primärer Domänen-Controller (nur für SMB-basierte Zielsysteme).
Profilserver	Server für die Einrichtung von Profilverzeichnissen für Benutzerkonten.
SAM Synchronisationsserver	Server für die Synchronisation mit einem SMB-basierten Zielsystem aus.
SMTP Host	Server, auf dem durch den One Identity Manager Service E-Mail Benachrichtigungen verschickt werden. Voraussetzung zum Versenden von Mails durch den One Identity Manager Service ist ein konfigurierter SMTP Host.
SQL Verarbeitung aktiviert (für Lastverteilung)	Der Server kann SQL Aufträge des DBQueue Prozessor ausführen (zur Lastverteilung). Ordnen Sie diese Funktion Jobservern zu, die nicht die Serverfunktion Master SQL Server besitzen. Das System verteilt die erzeugten Prozesse über diese Jobserver zusätzlich zum Master SQL Server.
Standard Berichtserver	Server, auf dem die Berichte generiert werden.
Windows PowerShell® Konnektor	Der Server kann Windows PowerShell® Version 3.0 oder neuer ausführen.

Verwandte Themen

- [Stammdaten eines Jobservers](#) auf Seite 56

Azure® Active Directory® Unternehmensverzeichnis

Ausführliche Informationen zur Azure® Active Directory® Struktur finden Sie in der Azure® Active Directory® Dokumentation von Microsoft.

Bei der erstmaligen Registrierung für einen Microsoft® Cloud-Dienst stellen Sie Details zu Ihrer Organisation bereit. Mit diesen Informationen wird eine neue Azure® Active Directory® Verzeichnisinstanz erstellt. Die Organisation repräsentiert einen Azure® Active Directory® Mandanten. Sie können im One Identity Manager einzelne Stammdaten des Mandanten bearbeiten. Neue Mandanten können Sie im One Identity Manager nicht erstellen.

Mit dem Unternehmensverzeichnis in der Cloud ist eine Basisdomäne verbunden. Zusätzlich können Sie im Azure® Active Directory® weitere benutzerdefinierte Domänen hinzufügen, welchen Sie dann die Microsoft® Cloud-Dienste zuordnen. One Identity Manager liest nur die Informationen verifizierter Domänen in die Datenbank ein. Die Bearbeitung der Informationen ist im One Identity Manager nicht möglich.

Detaillierte Informationen zum Thema

- [Azure® Active Directory® Mandant](#) auf Seite 60
- [Azure® Active Directory® Domänen](#) auf Seite 64

Azure® Active Directory® Mandant

Bei der erstmaligen Registrierung für einen Microsoft® Cloud-Dienst stellen Sie Details zu Ihrer Organisation bereit. Mit diesen Informationen wird eine neue Azure® Active Directory® Verzeichnisinstanz erstellt. Die Organisation repräsentiert einen Azure® Active Directory® Mandanten. Sie können im One Identity Manager einzelne Stammdaten des Mandanten bearbeiten. Neue Mandanten können Sie im One Identity Manager nicht erstellen.

Um die Stammdaten eines Azure® Active Directory® Mandanten zu bearbeiten

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


Detaillierte Informationen zum Thema

- [Allgemeine Stammdaten eines Azure® Active Directory® Mandanten auf Seite 61](#)
- [Informationen zum lokalen Active Directory® auf Seite 62](#)
- [Festlegen der Kategorien für die Vererbung von Berechtigungen auf Seite 63](#)

Allgemeine Stammdaten eines Azure® Active Directory® Mandanten

Auf dem Tabreiter **Allgemein** werden folgende Stammdaten abgebildet.

Tabelle 18: Stammdaten eines Mandanten

Eigenschaft	Beschreibung
Anzeigename	Anzeigename des Mandanten.
Kontendefinition (initial)	<p>Initiale Kontendefinition zur Erzeugung von Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für diesen Mandanten die automatische Zuordnung von Personen zu Benutzerkonten genutzt wird und dabei bereits verwaltete Benutzerkonten (Zustand "Linked configured") entstehen sollen. Es wird der Standardautomatisierungsgrad der Kontendefinition angewendet.</p> <p>Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand "Linked"). Dies ist beispielsweise bei der initialen Synchronisation der Fall.</p>
Zielsystemverantwortliche	<p>Anwendungsrolle, in der die Zielsystemverantwortlichen des Mandanten festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte des Mandanten, dem sie zugeordnet sind. Jedem Mandanten können somit andere Zielsystemverantwortliche zugeordnet werden.</p> <p>Wählen Sie die One Identity Manager Anwendungsrolle, deren Mitglieder verantwortlich für die Administration dieses Mandanten sind. Über die Schaltfläche  neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.</p>
Standort	Standort des Mandanten.
Straße	Straße.
Ort	Ort.
Postleitzahl	Postleitzahl.
Land	Land.

Eigenschaft	Beschreibung												
Synchronisiert durch	<p>HINWEIS: Die Art der Synchronisation können Sie nur festlegen, wenn Sie einen Mandanten neu anlegen. Nach dem Speichern sind keine Änderungen möglich.</p> <p>Beim Erstellen eines Mandanten mit dem Synchronization Editor wird "One Identity Manager" verwendet.</p> <p>Art der Synchronisation, über welche die Daten zwischen dem Mandanten und dem One Identity Manager synchronisiert werden.</p> <p>Tabelle 19: Zulässige Werte</p> <table border="1"> <thead> <tr> <th>Wert</th> <th>Synchronisation durch</th> <th>Provisionierung durch</th> </tr> </thead> <tbody> <tr> <td>One Identity Manager</td> <td>Azure® Active Directory® Konnektor</td> <td>Azure® Active Directory® Konnektor</td> </tr> <tr> <td>FIM</td> <td>Microsoft® Forefront® Identity Manager</td> <td>Microsoft® Forefront® Identity Manager</td> </tr> <tr> <td>Keine Synchronisation</td> <td>keine</td> <td>keine</td> </tr> </tbody> </table> <p>HINWEIS: Wenn Sie „Keine Synchronisation“ festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.</p>	Wert	Synchronisation durch	Provisionierung durch	One Identity Manager	Azure® Active Directory® Konnektor	Azure® Active Directory® Konnektor	FIM	Microsoft® Forefront® Identity Manager	Microsoft® Forefront® Identity Manager	Keine Synchronisation	keine	keine
Wert	Synchronisation durch	Provisionierung durch											
One Identity Manager	Azure® Active Directory® Konnektor	Azure® Active Directory® Konnektor											
FIM	Microsoft® Forefront® Identity Manager	Microsoft® Forefront® Identity Manager											
Keine Synchronisation	keine	keine											

Empfänger (Marketingbenachrichtigungen)	Liste von Empfängern von Marketingbenachrichtigungen.
Empfänger (Technische Benachrichtigungen)	Liste von Empfängern von technischen Benachrichtigungen.
Empfänger (Sicherheitsbenachrichtigungen)	Liste von Empfängern von Sicherheitsbenachrichtigungen.
Telefonnummern (Sicherheitsbenachrichtigungen)	Telefonnummern für Sicherheitsbenachrichtigung.

Verwandte Themen

- [Automatische Zuordnung von Personen zu Azure® Active Directory® Benutzerkonten](#) auf Seite 81
- [Zielsystemverantwortliche](#) auf Seite 53

Informationen zum lokalen Active Directory®

Auf dem Tabreiter **Verbund** werden folgende Informationen zum lokalen Active Directory®, welches mit dem Azure® Active Directory® Mandanten verbunden ist, abgebildet.


Tabelle 20: Angaben zum lokalen Active Directory® Benutzerkonto

Eigenschaft	Beschreibung
Synchronisation mit dem lokalen Active Directory® aktiviert	Angabe, ob die Synchronisation mit einem lokalen Active Directory® aktiviert ist.
Letzte Synchronisation	Zeitpunkt der letzten Synchronisation des Azure® Active Directory® Mandanten mit dem lokalen Active Directory®.

Festlegen der Kategorien für die Vererbung von Berechtigungen

Im One Identity Manager können Gruppen, Administratorrollen, Abonnements und unwirksame Dienstpläne selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen (Administratorrollen, Abonnements, unwirksame Dienstpläne) und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält verschiedene Tabellen. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In den übrigen Tabellen geben Sie Ihre Kategorien für die zielsystemabhängigen Gruppen, Administratorrollen, Abonnements und unwirksamen Dienstpläne an. Jede Tabelle enthält die Kategoriepositionen „Position 1“ bis „Position 31“.

Um Kategorien zu definieren

1. Wählen Sie die Kategorie **Azure® Active Directory® | Mandanten**.
2. Wählen Sie in der Ergebnisliste den Mandanten.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wechseln Sie auf den Tabreiter **Kategorien**.
5. Öffnen Sie den jeweiligen Basisknoten einer Tabelle.
6. Aktivieren Sie die Kategorie per Maus-Doppelklick auf das Symbol .
7. Tragen Sie eine beliebige Benennung der Kategorie für Benutzerkonten und Gruppen (Administratorrollen, Abonnements, unwirksamen Dienstpläne) in der verwendeten Anmeldesprache ein.
8. Speichern Sie die Änderungen.

Verwandte Themen

- [Vererbung von Azure® Active Directory® Gruppen anhand von Kategorien auf Seite 100](#)
- [Vererbung von Azure® Active Directory® Administratorrollen anhand von Kategorien auf Seite 112](#)
- [Vererbung von Azure® Active Directory® Abonnements anhand von Kategorien auf Seite 122](#)
- [Vererbung von unwirksamen Azure® Active Directory® Dienstplänen anhand von Kategorien auf Seite 130](#)

Synchronisationsprojekt bearbeiten

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

- ① **HINWEIS:** Der Manager ist währenddessen für die Bearbeitung gesperrt. Um Objekte im Manager bearbeiten zu können, schließen Sie den Synchronization Editor.

Um ein bestehendes Synchronisationsprojekt im Synchronization Editor zu öffnen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Mandanten**.
2. Wählen Sie in der Ergebnisliste den Mandanten. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten....**

Detaillierte Informationen zum Thema

- Ausführliche Informationen finden Sie im Dell One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation.

Verwandte Themen

- [Anpassen einer Synchronisationskonfiguration](#) auf Seite 24

Azure® Active Directory® Domänen

Mit dem Unternehmensverzeichnis in der Cloud ist eine Basisdomäne verbunden. Zusätzlich können Sie im Azure® Active Directory® weitere benutzerdefinierte Domänen hinzufügen, welchen Sie dann die Microsoft® Cloud-Dienste zuordnen. One Identity Manager liest nur die Informationen verifizierter Domänen in die Datenbank ein. Die Bearbeitung der Informationen ist im One Identity Manager nicht möglich.

Um einen Überblick über eine Domäne zu erhalten

1. Wählen Sie die Kategorie **Azure® Active Directory® | Verifizierte Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.
3. Wählen Sie die Aufgabe **Überblick über die Azure® Active Directory® Domäne**.

Tabelle 21: Stammdaten einer Domäne

Eigenschaft	Beschreibung
Name der Domäne	Vollständiger Name der Domäne.
Mandant	Mandant, zu dem diese Domäne eingetragen ist.
Typ	Typ der Domäne.

Eigenschaft	Beschreibung
Primäre Domäne	Angabe, ob es sich um die primäre Domäne handelt, beispielsweise zum Erstellen neuer Benutzerkonten.
Initiale Domäne	Angabe, ob es sich um die initiale Domäne handelt. Die initiale Domäne wird erstellt, wenn Sie einen Mandanten im Azure® Active Directory® registrieren.
Verfügbare Dienste	Liste der in dieser Domäne verfügbaren Dienste.

Azure® Active Directory® Benutzerkonten

Mit dem One Identity Manager verwalten Sie die Benutzerkonten einer Azure® Active Directory®-Umgebung. Um auf die Dienstpläne im Azure® Active Directory® zuzugreifen, benötigen die Benutzer ein Abonnement. Über die Mitgliedschaft in Gruppen erhalten die Benutzerkonten die nötigen Rechte zum Zugriff auf die Ressourcen.

Detaillierte Informationen zum Thema

- [Benutzerkonten mit Personen verbinden](#) auf Seite 66
- [Unterstützte Typen von Benutzerkonten](#) auf Seite 67
- [Erfassen der Stammdaten für Azure® Active Directory® Benutzerkonten](#) auf Seite 71

Benutzerkonten mit Personen verbinden

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

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

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

Wenn Sie Benutzerkonten über Kontendefinitionen verwalten, können Sie das Verhalten von Benutzerkonten beim Deaktivieren oder Löschen von Personen festlegen.

HINWEIS: Sollen Personen ihre Benutzerkonten über Kontendefinitionen erhalten, müssen die Personen ein zentrales Benutzerkonto besitzen und über die Zuordnung zu einer primären Abteilung, einem primären Standort oder einer primären Kostenstelle ihre IT Betriebsdaten erhalten.

- Beim Einfügen eines Benutzerkontos wird automatisch eine vorhandene Person zugeordnet oder im Bedarfsfall eine neue Person erstellt. Dabei werden die Personenstammdaten anhand vorhandener Benutzerkontenstammdaten erzeugt. Dieser Mechanismus kann eingesetzt werden, wenn eine neues Benutzerkonto manuell oder durch eine Synchronisation erstellt wird. Dieses Vorgehen ist jedoch nicht das Standardverfahren für den One Identity Manager. Für die automatische Personenzuordnung definieren Sie Kriterien, anhand derer die Personen ermittelt werden sollen.

Verwandte Themen

- [Erfassen der Stammdaten für Azure® Active Directory® Benutzerkonten](#) auf Seite 71
- [Einrichten von Kontendefinitionen](#) auf Seite 33
- [Automatische Zuordnung von Personen zu Azure® Active Directory® Benutzerkonten](#) auf Seite 81
- Ausführliche Informationen zur Behandlung und Administration von Personen und Benutzerkonten finden Sie im Dell One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

Unterstützte Typen von Benutzerkonten

Im One Identity Manager können unterschiedliche Typen von Benutzerkonten wie beispielsweise Standardbenutzerkonten, administrative Benutzerkonten oder Dienstkonten abgebildet werden. Zur Abbildung der verschiedenen Benutzerkontentypen werden die folgenden Eigenschaften verwendet.

- Identität (Spalte `IdentityType`)

Die Identität beschreibt den Typ des Benutzerkontos.

Tabelle 22: Identitäten von Benutzerkonten

Identität	Beschreibung	Wert der Spalte "IdentityType"
Primäre Identität	Standardbenutzerkonto einer Person.	Primary
Organisatorische Identität	Sekundäres Benutzerkonto, welches für unterschiedlichen Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen.	Organizational
Persönliche Administratoridentität	Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird.	Admin

Identität	Beschreibung	Wert der Spalte "IdentityType"
Zusatzidentität	Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird.	Sponsored
Gruppenidentität	Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird.	Shared
Dienstidentität	Dienstkonto.	Service

- Privilegiertes Benutzerkonto (Spalte `IsPrivilegedAccount`)

Mit dieser Option werden Benutzerkonten mit besonderen privilegierten Berechtigungen gekennzeichnet. Dazu gehören beispielsweise administrative Benutzerkonten oder Dienstkonten. Standardbenutzerkonten werden nicht mit dieser Option gekennzeichnet.

Standardbenutzerkonten

In der Regel erhält jede Person ein Standardbenutzerkonto, das die Berechtigungen besitzt, die für die tägliche Arbeit benötigt werden. Die Benutzerkonten haben eine Verbindung zur Person. Über eine Kontendefinition und deren Automatisierungsgrade kann die Auswirkung der Verbindung und der Umfang der vererbten Eigenschaften der Person an die Benutzerkonten konfiguriert werden.

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

- Unmanaged

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

- Full managed

Benutzerkonten mit dem Automatisierungsgrad „Full managed“ erben definierte Eigenschaften der zugeordneten Person.

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

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

Um Standardbenutzerkonten zu erstellen

1. Erstellen Sie eine Kontendefinition und weisen Sie die Automatisierungsgrade "Unmanaged" und "Full managed" zu.
2. Legen Sie für jeden Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll.

3. Erstellen Sie eine Abbildungsvorschrift für die IT Betriebsdaten.

Mit der Abbildungsvorschrift legen Sie fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden, beispielsweise ob der Container für ein Benutzerkonto über die Abteilung, die Kostenstelle, den Standort oder die Geschäftsrolle einer Person gebildet wird, und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über primären Rollen einer Person ermittelt werden können.

Welche IT Betriebsdaten erforderlich sind, ist abhängig vom Zielsystem. Für Standardbenutzerkonten werden folgende Einstellungen empfohlen:

- Verwenden Sie in der Abbildungsvorschrift für die Spalte `IsGroupAccount` den Standardwert "1" und aktivieren Sie die Option **Immer Standardwert verwenden**.
- Verwenden Sie in der Abbildungsvorschrift für die Spalte `IdentityType` den Standardwert "Primary" und aktivieren Sie die Option **Immer Standardwert verwenden**.

4. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem. Wählen Sie unter **Wirksam für** das konkrete Zielsystem.

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

5. Weisen Sie die Kontendefinition an die Personen zu.

Kontendefinitionen werden an die Personen des Unternehmens zugewiesen. Das Standardverfahren für die Zuweisung von Kontendefinitionen an Personen ist die indirekte Zuweisung. Die Kontendefinitionen werden an die Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen zugewiesen. Die Personen werden gemäß ihrer Funktion im Unternehmen in diese Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen eingeordnet und erhalten so ihre Kontendefinitionen. Um auf Sonderanforderungen zu reagieren, können einzelne Kontendefinitionen direkt an Personen zugewiesen werden. Kontendefinitionen können automatisch an alle Personen eines Unternehmens zugewiesen werden. Es ist möglich, die Kontendefinitionen als bestellbare Produkte dem IT Shop zuzuordnen. Der Abteilungsleiter kann dann für seine Mitarbeiter Benutzerkonten über das Web Portal bestellen. Zusätzlich ist es möglich, Kontendefinitionen in Systemrollen aufzunehmen. Diese Systemrollen können über hierarchische Rollen oder direkt an Personen zugewiesen werden oder als Produkte in den IT Shop aufgenommen werden.

Administrative Benutzerkonten

Für bestimmte administrative Aufgaben, ist der Einsatz administrativer Benutzerkonten notwendig. Administrative Benutzerkonten werden in der Regel vom Zielsystem vorgegeben und haben feste Bezeichnungen und Anmeldenamen, wie beispielsweise "Administrator".

Administrative Benutzerkonten werden durch die Synchronisation in den One Identity Manager eingelesen. Um administrativen Benutzerkonten einen Verantwortlichen zuzuweisen, weisen Sie dem Benutzerkonto im One Identity Manager eine Person zu.

Privilegierte Benutzerkonten

Privilegierte Benutzerkonten werden eingesetzt, um Personen mit zusätzlichen privilegierten Berechtigungen auszustatten.

Um privilegierte Benutzerkonten zu erstellen

1. Erstellen Sie eine Kontendefinition. Erstellen Sie einen neuen Automatisierungsgrad für privilegierte Benutzerkonten und weisen Sie diesen Automatisierungsgrad an die Kontendefinition zu.
2. Wenn Sie verhindern möchten, dass die Eigenschaften für privilegierte Benutzerkonten überschrieben werden, setzen Sie für den Automatisierungsgrad die Eigenschaft **IT Betriebsdaten überschreibend** auf den Wert "Nur initial". In diesem Fall werden die Eigenschaften einmalig beim Erstellen der Benutzerkonten befüllt.
3. Legen Sie für den Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll.
4. Erstellen Sie eine Abbildungsvorschrift für die IT Betriebsdaten.

Mit der Abbildungsvorschrift legen Sie fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden, beispielsweise ob der Container für ein Benutzerkonto über die Abteilung, die Kostenstelle, den Standort oder die Geschäftsrolle einer Person gebildet wird, und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über primären Rollen einer Person ermittelt werden können.

Welche IT Betriebsdaten erforderlich sind, ist abhängig vom Zielsystem. Für privilegierte Benutzerkonten werden folgende Einstellungen empfohlen:

- Verwenden Sie in der Abbildungsvorschrift für die Spalte `IsPrivilegedAccount` den Standardwert "1" und aktivieren Sie die Option **Immer Standardwert verwenden**.
 - Zusätzlich können Sie eine Abbildungsvorschrift für die Spalte `IdentityType` festlegen. Die Spalte besitzt verschiedene zulässige Werte, die privilegierte Benutzerkonten repräsentieren.
 - Um zu verhindern, dass privilegierte Benutzerkonten Gruppen des Standardbenutzers erben, definieren Sie eine Abbildungsvorschrift für die Spalte `IsGroupAccount` mit dem Standardwert "0" und aktivieren Sie die Option **Immer Standardwert verwenden**.
5. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem.

Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.

6. Weisen Sie die Kontendefinition direkt an die Personen zu, die mit privilegierten Benutzerkonten arbeiten sollen.

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

- HINWEIS:** Administrative Benutzerkonten können automatisch als privilegierte Benutzerkonten gekennzeichnet werden. Aktivieren Sie dazu im Designer den Zeitplan "Ausgewählte Benutzerkonten als privilegiert kennzeichnen".

Die Kriterien anhand derer Benutzerkonten automatisch als privilegiert erkannt werden, sind als Erweiterungen zur Sichtdefinition (ViewAddOn) an der Tabelle `TSBVAccountIsPrivDetectRule` (Tabelle vom Typ "Union") definiert. Die Auswertung erfolgt im Skript `TSB_SetIsPrivilegedAccount`. Die Benutzerkonten werden mit der Eigenschaft **Privilegiertes Benutzerkonto** (`IsPrivilegedAccount`) gekennzeichnet.

- ① **HINWEIS:** Wenn es unternehmensspezifisch erforderlich ist, dass die Anmeldenamen privilegierter Benutzerkonten einen definierten Namensschema folgen, legen Sie die Bildungsregel fest, nach denen Anmeldenamen gebildet werden.

Um ein Präfix für den Anmeldenamen zu verwenden, aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\AzureAD\Accounts\PrivilegedAccount\AccountName_Prefix".
Um ein Postfix für den Anmeldenamen zu verwenden, aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\AzureAD\Accounts\PrivilegedAccount\AccountName_Postfix".


Diese Konfigurationsparameter werden in der Standardinstallation ausgewertet, wenn Sie ein Benutzerkonto, mit der Eigenschaft **Privilegiertes Benutzerkonto** (`IsPrivilegedAccount`) kennzeichnen. Die Anmeldenamen der Benutzerkonten werden entsprechend der Bildungsregeln umbenannt. Dies erfolgt auch, wenn die Benutzerkonten über den Zeitplan "Ausgewählte Benutzerkonten als privilegiert kennzeichnen" als privilegiert gekennzeichnet werden.

Erfassen der Stammdaten für Azure® Active Directory® Benutzerkonten

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

- ① **HINWEIS:** Um Benutzerkonten für die Personen eines Unternehmens einzurichten, wird der Einsatz von Kontendefinitionen empfohlen. Einige der nachfolgend beschriebenen Stammdaten werden dabei über Bildungsregeln aus den Personenstammdaten gebildet.
- ① **HINWEIS:** Sollen Personen ihre Benutzerkonten über Kontendefinitionen erhalten, müssen die Personen ein zentrales Benutzerkonto besitzen und über die Zuordnung zu einer primären Abteilung, einem primären Standort oder einer primären Kostenstelle ihre IT Betriebsdaten erhalten.
- ① **TIPP:** Damit eine Person automatisiert ein Benutzerkonto und ein Abonnement erhält, können Sie die Kontendefinition zur Erstellung des Benutzerkontos und das zu verwendende Abonnement in einer Systemrolle zusammenfassen.
- Eine Person kann diese Systemrolle direkt erhalten, über Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen erben oder über den IT Shop bestellen.

Um die Stammdaten eines Benutzerkontos zu bearbeiten

1. Wählen Sie die Kategorie **Azure® Active Directory® | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
- ODER -
Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

Um ein Benutzerkonto für eine Person manuell zuzuweisen oder zu erstellen

1. Wählen Sie die Kategorie **Personen** | **Personen**.
2. Wählen Sie in der Ergebnisliste die Person und führen Sie die Aufgabe **Azure® Active Directory® Benutzerkonten zuweisen** aus.
3. Weisen Sie ein Benutzerkonto zu.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- [Allgemeine Stammdaten eines Azure® Active Directory® Benutzerkontos](#) auf Seite 72
- [Kontaktdaten eines Azure® Active Directory® Benutzerkontos](#) auf Seite 75
- [Organisatorische Informationen eines Azure® Active Directory® Benutzerkontos](#) auf Seite 75
- [Informationen zum lokalen Active Directory® Benutzerkonto](#) auf Seite 76

Verwandte Themen


- [Einrichten von Kontendefinitionen](#) auf Seite 33
- [Unterstützte Typen von Benutzerkonten](#) auf Seite 67
- [Azure® Active Directory® Abonnements und Dienstpläne](#) auf Seite 113

Allgemeine Stammdaten eines Azure® Active Directory® Benutzerkontos

Auf dem Tabreiter **Allgemein** erfassen Sie folgende Stammdaten.

Tabelle 23: Allgemeine Stammdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Person	Person, die das Benutzerkonto verwendet. Wurde das Benutzerkonto über eine Kontendefinition erzeugt, ist die Person bereits eingetragen. Wenn Sie das Benutzerkonto manuell erstellen, können Sie die Person aus der Auswahlliste wählen. Wenn Sie die automatische Personenzuordnung nutzen, wird beim Speichern des Benutzerkontos eine zugehörige Person erzeugt und in das Benutzerkonto übernommen.

Eigenschaft	Beschreibung
Kontendefinition	<p>Kontendefinition, über die das Benutzerkonto erstellt wurde.</p> <p>Die Kontendefinition wird benutzt, um die Stammdaten des Benutzerkontos automatisch zu befüllen und um einen Automatisierungsgrad für das Benutzerkonto festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Person und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein.</p> <p> HINWEIS: Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden.</p> <p>Um das Benutzerkonto manuell über eine Kontendefinition zu erstellen, tragen Sie im Eingabefeld Person eine Person ein. Es können alle Kontendefinitionen ausgewählt werden, die dieser Person zugewiesen sind und über die noch kein Benutzerkonto für diese Person erstellt wurde.</p>
Automatisierungsgrad	Automatisierungsgrad des Benutzerkontos. Wählen Sie einen Automatisierungsgrad aus der Auswahlliste. Den Automatisierungsgrad können Sie nur festlegen, wenn Sie auch eine Kontendefinition eingetragen haben. In der Auswahlliste werden alle Automatisierungsgrade der gewählten Kontendefinition angeboten.
Mandant	Mandant des Benutzerkontos.
Domäne	Domäne des Benutzerkontos.
Standort	Standort, an dem das Benutzerkonto genutzt wird.
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 Automatisierungsgrad automatisch ausgefüllt.
Benutzeranmeldename	Anmeldename des Benutzerkontos. Der Benutzeranmeldename wird gebildet aus dem Alias und der Domäne. Der Benutzeranmeldename entspricht dem Benutzernamen (User Principal Name) des Benutzers im Azure® Active Directory®.
Alias	E-Mail Alias für das Benutzerkonto.
Bevorzugte Sprache	Bevorzugte Sprache des Benutzers, beispielsweise "en-US".
Kennwort	Kennwort für das Benutzerkonto. Abhängig vom Konfigurationsparameter "Person\UseCentralPassword" wird das zentrale Kennwort der zugeordneten Person auf das Kennwort des Benutzerkontos abgebildet. Wenn Sie ein initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen.
Kennwortbestätigung	Kennwortwiederholung.
Kennwort bei der nächsten Anmeldung ändern	Angabe, ob der Benutzer bei der nächsten Anmeldung das Kennwort anpassen muss.

Eigenschaft	Beschreibung														
Kennwortrichtlinien	Kennwortrichtlinien, die für das Benutzerkonto gelten. Zur Verfügung stehen die Optionen Keine Einschränkungen , Kennwort läuft nie ab und Schwache Kennwörter zulassen .														
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten . Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter „QER\CalculateRiskIndex“ aktiviert ist. Ausführliche Informationen finden Sie im Dell One Identity Manager Administrationshandbuch für Risikobewertungen.														
Kategorie	Kategorien für die Vererbung von Gruppen an das Benutzerkonto. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien. Gruppen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt.														
Identität	<p>Typ der Identität des Benutzerkontos.</p> <p>Tabelle 24: Zulässige Werte für die Identität</p> <table border="1"> <thead> <tr> <th>Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>Primäre Identität</td> <td>Standardbenutzerkonto einer Person.</td> </tr> <tr> <td>Organisatorische Identität</td> <td>Sekundäres Benutzerkonto, welches für unterschiedlichen Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen.</td> </tr> <tr> <td>Persönliche Administratoridentität</td> <td>Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird.</td> </tr> <tr> <td>Zusatzidentität</td> <td>Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird.</td> </tr> <tr> <td>Gruppenidentität</td> <td>Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird.</td> </tr> <tr> <td>Dienstidentität</td> <td>Dienstkonto.</td> </tr> </tbody> </table>	Wert	Beschreibung	Primäre Identität	Standardbenutzerkonto einer Person.	Organisatorische Identität	Sekundäres Benutzerkonto, welches für unterschiedlichen Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen.	Persönliche Administratoridentität	Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird.	Zusatzidentität	Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird.	Gruppenidentität	Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird.	Dienstidentität	Dienstkonto.
Wert	Beschreibung														
Primäre Identität	Standardbenutzerkonto einer Person.														
Organisatorische Identität	Sekundäres Benutzerkonto, welches für unterschiedlichen Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen.														
Persönliche Administratoridentität	Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird.														
Zusatzidentität	Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird.														
Gruppenidentität	Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird.														
Dienstidentität	Dienstkonto.														
Privilegiertes Benutzerkonto	Angabe, ob es sich um ein privilegiertes Benutzerkonto handelt.														
Gruppen erbbar	<p>Angabe, ob das Benutzerkonto Gruppen über die Person erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt.</p> <ul style="list-style-type: none"> • Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Person eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Gruppe nur, wenn die Option aktiviert ist. 														
Benutzerkonto ist deaktiviert	Angabe, ob das Benutzerkonto deaktiviert ist. Wird ein Benutzerkonto vorübergehend nicht benötigt, können Sie das Benutzerkonto über die Option zeitweilig deaktivieren.														

Verwandte Themen

- [Einrichten von Kontendefinitionen auf Seite 33](#)
- [Vererbung von Azure® Active Directory® Gruppen anhand von Kategorien auf Seite 100](#)
- [Benutzerkonten mit Personen verbinden auf Seite 66](#)
- [Unterstützte Typen von Benutzerkonten auf Seite 67](#)
- [Deaktivieren von Azure® Active Directory® Benutzerkonten auf Seite 85](#)

Kontaktdaten eines Azure® Active Directory® Benutzerkontos

Auf dem Tabreiter **Kontakt** erfassen Sie folgende Adressinformationen zur Erreichbarkeit der Person, die das Benutzerkonto verwendet.

Tabelle 25: Kontaktdaten

Eigenschaft	Beschreibung
Straße	Straße. 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.
Ort	Ort. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. Anhand des Ortes können automatisch Standorte erzeugt und den Personen zugeordnet werden.
Postleitzahl	Postleitzahl. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Land	Länderkennung.
Geschäftstelefone	Geschäftliche Telefonnummern.
Mobiltelefon	Mobiltelefonnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
E-Mail-Adresse	E-Mail-Adresse des Benutzers.
Proxy Adressen	Weitere E-Mail-Adressen des Benutzers. Als Adresstyp können Sie zusätzlich zur Standardadressierung (SMTP, X400) weitere Mailkonnektoren (beispielsweise CCMail, MS) nutzen. Für die Erstellung weiterer Proxy Adressen ist die folgende Syntax einzuhalten: <code>Adresstyp: neue E-Mail-Adresse</code>


Organisatorische Informationen eines Azure® Active Directory® Benutzerkontos

Auf dem Tabreiter **Organisatorisch** erfassen Sie folgende organisatorischen Stammdaten.

Tabelle 26: Organisatorische Stammdaten

Eigenschaft	Beschreibung
Büro	Büro. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Firma	Firma der Person. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Abteilung	Abteilung der Person. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. Anhand der Abteilungsinformation können automatisch Abteilungen erzeugt und den Personen zugeordnet werden.
Berufsbezeichnung	Berufsbezeichnung. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Kontomanager	Verantwortlicher für das Benutzerkonto.

Um einen Kontomanager 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**.

Informationen zum lokalen Active Directory® Benutzerkonto

Auf dem Tabreiter **Verbund** werden folgende Informationen zum lokalen Active Directory® Benutzerkonto, welches mit dem Azure® Active Directory® Benutzerkonto verbunden ist, abgebildet.

Tabelle 27: Angaben zum lokalen Active Directory® Benutzerkonto

Eigenschaft	Beschreibung
Synchronisation mit dem lokalen Active Directory® aktiviert	Angabe, ob die Synchronisation mit einem lokalen Active Directory® aktiviert ist.
Letzte Synchronisation	Zeitpunkt der letzten Synchronisation des Azure® Active Directory® Benutzerkontos mit dem lokalen Active Directory®.
SID des lokalen Kontos	Sicherheits-ID (SID) des lokalen Active Directory® Benutzerkontos.
Unveränderlicher Bezeichner	Unveränderlicher Bezeichner, mit dem die Beziehung zwischen Active Directory® und Azure® Active Directory® aufrechterhalten wird.

Zusätzliche Aufgaben für die Verwaltung von Azure® Active Directory® Benutzerkonten

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können.

Überblick über das Azure® Active Directory® Benutzerkonto

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einem Benutzerkonto.

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie die Kategorie **Azure® Active Directory® | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das Azure® Active Directory® Benutzerkonto**.

Verwandte Themen

- [Azure® Active Directory® Abonnements und Dienstpläne auf Seite 113](#)

Ändern des Automatisierungsgrades an einem Azure® Active Directory® Benutzerkonto

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

Um den Automatisierungsgrad für ein Benutzerkonto zu ändern

1. Wählen Sie die Kategorie **Azure® Active Directory® | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Automatisierungsgrad** den Automatisierungsgrad.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Erfassen der Stammdaten für Azure® Active Directory® Benutzerkonten auf Seite 71](#)

Azure® Active Directory® Gruppen direkt an ein Azure® Active Directory® Benutzerkonto zuweisen

Gruppen können einem Benutzerkonto direkt oder indirekt zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der Gruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person ein Benutzerkonto im Azure® Active Directory®, werden die Gruppen der Rollen an dieses Benutzerkonto vererbt.

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

Um Gruppen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Gruppe an Azure® Active Directory® Benutzerkonten zuweisen](#) auf Seite 91

Azure® Active Directory® Administratorrollen direkt an ein Azure® Active Directory® Benutzerkonto zuweisen

Administratorrollen können einem Benutzerkonto direkt oder indirekt zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der Administratorrollen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person ein Benutzerkonto im Azure® Active Directory®, werden die Administratorrollen der Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen an dieses Benutzerkonto vererbt.

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

Um Administratorrollen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Administratorrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Administratorrollen zu.

- ODER -

Entfernen Sie im Bereich **Zuordnungen entfernen** die Administratorrollen.

5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Administratorrollen an Azure® Active Directory® Benutzerkonten zuweisen auf Seite 105](#)

Azure® Active Directory® Abonnements direkt an Azure® Active Directory® Benutzerkonten zuweisen

Abonnements können Sie einem Benutzerkonto direkt oder indirekt zuweisen. Bei der indirekten Zuweisung werden Personen und Abonnements in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Besitzt die Person ein Benutzerkonto im Azure® Active Directory®, werden die Abonnements der Rollen an dieses Benutzerkonto vererbt.

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

Um Abonnements direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Abonnements zuweisen**.
4. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Abonnements an Azure® Active Directory® Benutzerkonten zuweisen auf Seite 115](#)

Unwirksamen Azure® Active Directory® Dienstpläne direkt an Azure® Active Directory® Benutzerkonten zuweisen

Unwirksame Dienstpläne können Sie einem Benutzerkonto direkt oder indirekt zuweisen. Bei der indirekten Zuweisung werden Personen und unwirksame Dienstpläne in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Besitzt die Person ein Benutzerkonto im Azure® Active Directory®, werden die unwirksamen Dienstpläne der Rollen an dieses Benutzerkonto vererbt.

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

Um unwirksame Dienstpläne direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Unwirksame Dienstpläne zuweisen**.
4. Speichern Sie die Änderungen.

Verwandte Themen

- [Unwirksame Azure® Active Directory® Dienstpläne an Azure® Active Directory® Benutzerkonten zuweisen](#) auf Seite 124

Zusatzeigenschaften an ein Azure® Active Directory® Benutzerkonto zuweisen

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

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Zusatzeigenschaften.
5. Speichern Sie die Änderungen.

Verwandte Themen

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

Automatische Zuordnung von Personen zu Azure® Active Directory® Benutzerkonten

Tabelle 28: Konfigurationsparameter für die automatische Personenzuordnung

Konfigurationsparameter	Bedeutung
TargetSystem\AzureAD\PersonAutoFullsync	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem\AzureAD\PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem\AzureAD\PersonExcludeList	Der Konfigurationsparameter enthält eine Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe () getrennten Liste, die als reguläres Suchmuster verarbeitet wird. Beispiel: ADMINISTRATOR
TargetSystem\AzureAD\ PersonAutoDisabledAccounts	Der Konfigurationsparameter legt fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.

Beim Einfügen eines Benutzerkontos kann automatisch eine vorhandene Person zugeordnet und im Bedarfsfall neu erstellt werden. Dabei werden die Personenstammdaten anhand vorhandener Benutzerstammdaten erzeugt. Dieser Mechanismus kann auf die Erstellung eines neuen Benutzerkontos durch manuelle Anlage oder Synchronisation folgen. Für die automatische Personenzuordnung definieren Sie Kriterien für die Ermittlung der Personen. Wird durch den eingesetzten Modus ein Benutzerkonto mit einer Person verbunden, so erhält das Benutzerkonto durch interne Verarbeitung den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Abhängig davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden.

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

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

Führen Sie folgende Aktionen aus, damit Personen automatisch zugeordnet werden können.

- Wenn Personen bei der Synchronisation von Benutzerkonten zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter „TargetSystem\AzureAD\PersonAutoFullsync“ und wählen Sie den gewünschte Modus.
- Wenn Personen außerhalb der Synchronisation zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter „TargetSystem\AzureAD\PersonAutoDefault“ und wählen Sie den gewünschte Modus.
- Legen Sie im Konfigurationsparameter "TargetSystem\AzureAD\PersonExcludeList" die Benutzerkonten fest, für die keine automatische Zuordnung zu Personen erfolgen soll.

Beispiel:

ADMINISTRATOR

- Legen Sie über den Konfigurationsparameter "TargetSystem\AzureAD\PersonAutoDisabledAccounts" fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
- Weisen Sie der Domäne eine Kontendefinition zu. Stellen Sie sicher, dass der Automatisierungsgrad, der verwendet werden soll, als Standardautomatisierungsgrad eingetragen ist.
- Definieren Sie die Suchkriterien für die Personenzuordnung an der Domäne.

HINWEIS:

Für die Synchronisation gilt:

- Die automatische Personenzuordnung wirkt, wenn Benutzerkonten neu angelegt oder aktualisiert werden.

Außerhalb der Synchronisation gilt:

- Die automatische Personenzuordnung wirkt, wenn Benutzerkonten neu angelegt werden.

- HINWEIS:** Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Personen erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für den Mandanten bekannt, werden die Benutzerkonten mit den Personen verbunden. Es wird jedoch noch keine Kontendefinition zugewiesen. Die Benutzerkonten sind somit im Zustand "Linked" (verbunden).

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie dem Mandanten eine Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand "Linked" (verbunden) die Kontendefinition und den Automatisierungsgrad zu.
 - a. Wählen Sie die Kategorie **Azure® Active Directory® | Benutzerkonten | Verbunden aber nicht konfiguriert | <Mandant>**.
 - b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.

Verwandte Themen

- [Erstellen einer Kontendefinition](#) auf Seite 34
- [Zuweisen der Kontendefinition an ein Zielsystem](#) auf Seite 48
- [Bearbeiten der Suchkriterien für die automatische Personenzuordnung](#) auf Seite 83

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

Bearbeiten der Suchkriterien für die automatische Personenzuordnung

Die Kriterien für die Personenzuordnung werden am Mandanten definiert. Dabei legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person dem Benutzerkonto zugeordnet werden kann. Die Suchkriterien können Sie durch Formatdefinitionen weiter einschränken. Das zusammengestellte Suchkriterium wird in XML-Notation in die Spalte „Suchkriterien für die automatische Personenzuordnung“ (AccountToPersonMatchingRule) der Tabelle `AADOrganization` geschrieben.

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

- ① **HINWEIS:** Bei der Zuordnung der Personen zu Benutzerkonten anhand der Suchkriterien erhalten die Benutzerkonten den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Abhängig davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden. Für administrative Benutzerkonten wird empfohlen, die Zuordnung nicht anhand der Suchkriterien vorzunehmen. Ordnen Sie Personen zu administrativen Benutzerkonten über die Aufgabe **Stammdaten bearbeiten** am jeweiligen Benutzerkonto zu.
- ① **HINWEIS:** Der One Identity Manager liefert ein Standardmapping für die Personenzuordnung. Führen Sie die folgenden Schritte nur aus, wenn Sie das Standardmapping unternehmensspezifisch anpassen möchten.

Um Kriterien für die Personenzuordnung festzulegen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Mandanten**.
2. Wählen Sie in der Ergebnisliste den Mandanten.
3. Wählen Sie die Aufgabe **Suchkriterien für die Personenzuordnung definieren**.
4. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person mit dem Benutzerkonto verbunden wird.

Tabelle 29: Standardsuchkriterien für Benutzerkonten und Kontakte

Anwenden auf	Spalte an Person	Spalte am Benutzerkonto
Azure® Active Directory® Benutzerkonten	Zentrales Benutzerkonto (CentralAccount)	Alias (MailNickName)


5. Speichern Sie die Änderungen.

Direkte Zuordnung von Personen an Benutzerkonten anhand einer Vorschlagsliste

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

Tabelle 30: Ansichten zur manuellen Zuordnung

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

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

Um die Suchkriterien auf die Benutzerkonten anzuwenden

- Klicken Sie **Neu laden**.

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

Um Personen direkt über die Vorschlagsliste zuzuordnen

1. Klicken Sie **Vorgeschlagene Zuordnungen**.

- a. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die vorgeschlagene Person zugeordnet werden soll. Eine Mehrfachauswahl ist möglich.
- b. Klicken Sie **Ausgewählte zuweisen**.
- c. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Den ausgewählten Benutzerkonten werden die per Suchkriterium ermittelten Personen zugeordnet.

- ODER -

2. Klicken Sie **Ohne Personenzuordnung**.

- a. Klicken Sie **Person auswählen...** für das Benutzerkonto, dem eine Person zugeordnet werden soll. Wählen Sie eine Person aus der Auswahlliste.
- b. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die ausgewählten Personen zugeordnet werden sollen. Eine Mehrfachauswahl ist möglich.
- c. Klicken Sie **Ausgewählte zuweisen**.
- d. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Den ausgewählten Benutzerkonten werden die Personen zugeordnet, die in der Spalte "Person" angezeigt werden.

Um Zuordnungen zu entfernen

1. Klicken Sie **Zugeordnete Benutzerkonten**.

- a. Klicken Sie **Auswahl** für alle Benutzerkonten, deren Personenzuordnung entfernt werden soll. Mehrfachauswahl ist möglich.
- b. Klicken Sie **Ausgewählte entfernen**.

- c. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Von den ausgewählten Benutzerkonten werden die zugeordneten Personen entfernt.

Detaillierte Informationen zum Thema

- Ausführliche Informationen zur automatische Zuordnung von Personen zu Benutzerkonten finden Sie im Dell One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

Verwandte Themen

- [Automatische Zuordnung von Personen zu Azure® Active Directory® Benutzerkonten](#) auf Seite 81

Deaktivieren von Azure® Active Directory® Benutzerkonten

Tabelle 31: Konfigurationsparameter für das von Benutzerkonten

Konfigurationsparameter	Bedeutung
QER\Person\TemporaryDeactivation	Der Konfigurationsparameter legt fest, ob die Benutzerkonten der Person gesperrt werden, wenn die Person zeitweilig oder dauerhaft deaktiviert wird.

Wie Sie Benutzerkonten deaktivieren, ist abhängig von der Art der Verwaltung der Benutzerkonten.

Szenario:

- Die Benutzerkonten sind mit Personen verbunden und werden über Kontendefinitionen verwaltet.

Benutzerkonten, die über Kontendefinitionen verwaltet werden, werden deaktiviert, wenn die Person dauerhaft oder zeitweilig deaktiviert wird. Das Verhalten ist abhängig vom Automatisierungsgrad des Benutzerkontos. Benutzerkonten mit dem Automatisierungsgrad „Full managed“ werden entsprechend der Einstellungen an der Kontendefinition deaktiviert. Für Benutzerkonten mit einem anderen Automatisierungsgrad konfigurieren Sie das gewünschte Verhalten an der Bildungsregel der Spalte `AADUser.AccountDisabled`.

Szenario:

- Die Benutzerkonten sind mit Personen verbunden. Es sind keine Kontendefinitionen zugeordnet.

Benutzerkonten, die mit Personen verbunden sind, jedoch nicht über Kontendefinitionen verwaltet werden, werden deaktiviert, wenn die Person dauerhaft oder zeitweilig deaktiviert wird. Das Verhalten ist abhängig vom Konfigurationsparameter "QER\Person\TemporaryDeactivation".

- Ist der Konfigurationsparameter aktiviert, werden die Benutzerkonten einer Person deaktiviert, wenn die Person zeitweilig oder dauerhaft deaktiviert wird.
- Ist der Konfigurationsparameter deaktiviert, haben die Eigenschaften der Person keinen Einfluss auf die verbundenen Benutzerkonten.

Um das Benutzerkonto bei deaktiviertem Konfigurationsparameter zu sperren

1. Wählen Sie die Kategorie **Azure® Active Directory® | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Benutzerkonto ist deaktiviert**.
5. Speichern Sie die Änderungen.

Szenario:

- Benutzerkonten sind nicht mit Personen verbunden.

Um ein Benutzerkonto zu sperren, das nicht mit einer Person verbunden ist

1. Wählen Sie die Kategorie **Azure® Active Directory® | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Benutzerkonto ist deaktiviert**.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Einrichten von Kontendefinitionen](#) auf Seite 33
- [Erstellen der Automatisierungsgrade](#) auf Seite 36
- [Löschen und Wiederherstellen von Azure® Active Directory® Benutzerkonten](#) auf Seite 86
- Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im Dell One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

Löschen und Wiederherstellen von Azure® Active Directory® Benutzerkonten

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

Um ein Benutzerkonto zu löschen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Löschen Sie das Benutzerkonto.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Um ein Benutzerkonto wiederherzustellen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste die Schaltfläche **Löschen rückgängig machen**.

Konfigurieren der Löschverzögerung

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

Verwandte Themen

- [Deaktivieren von Azure® Active Directory® Benutzerkonten auf Seite 85](#)
- Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im Dell One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

Azure® Active Directory® Gruppen

Azure® Active Directory® kennt verschiedene Gruppentypen, in denen Benutzer und Gruppen zusammengefasst werden können, um beispielsweise den Zugriff auf Ressourcen oder die Verteilung von E-Mails zu regeln.

Gruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können einzelne Stammdaten der Gruppen bearbeiten. Im One Identity Manager können Sie neue Sicherheitsgruppen erstellen. Andere Gruppentypen können Sie im One Identity Manager nicht erstellen.

Um Benutzer in Gruppen aufzunehmen, können Sie die Gruppen direkt an die Benutzer zuweisen. Sie können Gruppen an Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder den IT Shop zuweisen.

Nachfolgend sind die im One Identity Manager unterstützten Gruppentypen aufgeführt.

Tabelle 32: Unterstützte Gruppentypen

Gruppentyp	Beschreibung
Sicherheitsgruppe	<p>Über Sicherheitsgruppen werden Berechtigungen auf Ressourcen erteilt. In Sicherheitsgruppen werden Benutzerkonten und andere Gruppen aufgenommen und somit die Administration erleichtert.</p> <p>Sicherheitsgruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können im One Identity Manager Sicherheitsgruppen bearbeiten sowie neue Sicherheitsgruppen erstellen.</p>
Office 365 Gruppe	<p>Office 365 Gruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können im One Identity Manager Office 365 Gruppen bearbeiten. Neue Office 365 Gruppen können Sie im One Identity Manager nicht erstellen.</p>
Verteilerguppe	<p>Verteilerguppen werden eingesetzt, um E-Mails an die Mitglieder der Gruppe zu versenden. Verteilerguppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können im One Identity Manager Verteilerguppen bearbeiten. Neue Verteilerguppen können Sie im One Identity Manager nicht erstellen.</p>
E-Mail aktivierte Sicherheitsgruppe	<p>E-Mail aktivierte Sicherheitsgruppen sind Sicherheitsgruppen, die als Verteilerguppen eingesetzt werden.</p> <p>E-Mail aktivierte Sicherheitsgruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können im One Identity Manager E-Mail aktivierte Sicherheitsgruppen bearbeiten. Neue E-Mail aktivierte Sicherheitsgruppen können Sie im One Identity Manager nicht erstellen.</p>


Verwandte Themen

- [Bearbeiten der Stammdaten von Azure® Active Directory® Gruppen auf Seite 89](#)

Bearbeiten der Stammdaten von Azure® Active Directory® Gruppen

Gruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können im One Identity Manager neue Sicherheitsgruppen erstellen. Andere Gruppentypen können Sie lediglich bearbeiten. Welche Stammdaten einer Gruppe Sie bearbeiten können, ist abhängig vom Gruppentyp.

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie die Kategorie **Azure® Active Directory® | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
- ODER -
Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten für eine Gruppe.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- [Allgemeine Stammdaten einer Azure® Active Directory® Gruppe auf Seite 89](#)
- [Informationen zur lokalen Active Directory® Gruppe auf Seite 90](#)

Allgemeine Stammdaten einer Azure® Active Directory® Gruppe

Auf dem Tabreiter **Allgemein** erfassen Sie folgende Stammdaten.

Tabelle 33: Allgemeine Stammdaten

Eigenschaft	Beschreibung
Anzeigename	Anzeigename zur Anzeige der Gruppe in der Benutzeroberfläche der One Identity Manager Werkzeuge.
Mandant	Mandant der Gruppe.
Alias	E-Mail Alias für die Gruppe.
E-Mail-Adresse	E-Mail-Adresse der Gruppe.
Proxy Adressen	Weitere E-Mail-Adressen der Gruppe. Als Adresstyp können Sie zusätzlich zur Standardadressierung (SMTP, X400) weitere Mailkonnektoren (beispielsweise CCMail, MS) nutzen. Für die Erstellung weiterer Proxy Adressen ist die folgende Syntax einzuhalten: Adresstyp: neue E-Mail-Adresse
Gruppentyp	Angabe des Typs einer Gruppe. Für Office 365 Gruppen ist der Wert "Unified" eingetragen. Für Sicherheitsgruppen und Verteilergruppen ist der Wert leer.

Eigenschaft	Beschreibung
Sicherheitsgruppe	Angabe, ob es sich um eine Sicherheitsgruppe handelt. Über Sicherheitsgruppen werden Berechtigungen auf Ressourcen erteilt. In Sicherheitsgruppen werden Benutzerkonten und andere Gruppen aufgenommen und somit die Administration erleichtert.
E-Mail aktiviert	Angabe, ob für die Gruppe E-Mail aktiviert ist. Ist die Option für eine Sicherheitsgruppe gesetzt, dann handelt es sich um eine E-Mail aktivierte Sicherheitsgruppe. Anderenfalls handelt es sich um eine Verteilergruppe.
IT Shop	Angabe, ob die Gruppe über den IT Shop bestellbar ist. Die Gruppe kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Die Gruppe kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen ist nicht zulässig.
Leistungsposition	Angabe einer Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter „QER\CalculateRiskIndex“ aktiviert ist.
Kategorie	Kategorien für die Vererbung von Gruppen. Gruppen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Über die Auswahlliste ordnen Sie die Gruppe einer oder mehreren Kategorien zu.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Verwandte Themen

- [Vererbung von Azure® Active Directory® Gruppen anhand von Kategorien](#) auf Seite 100
- Ausführliche Informationen zur Risikobewertung finden Sie im Dell One Identity Manager Administrationshandbuch für Risikobewertungen.
- Ausführliche Informationen zur Vorbereitung der Gruppen für die Bestellung über den IT Shop finden Sie im Dell One Identity Manager Administrationshandbuch für IT Shop.

Informationen zur lokalen Active Directory® Gruppe

Auf dem Tabreiter **Verbund** werden folgende Informationen zur lokalen Active Directory® Gruppe, welche mit der Azure® Active Directory® Gruppe verbunden ist, abgebildet.

Tabelle 34: Angaben zur lokalen Active Directory® Gruppe

Eigenschaft	Beschreibung
Synchronisation mit dem lokalen Active Directory® aktiviert	Angabe, ob die Synchronisation mit einem lokalen Active Directory® aktiviert ist.
Letzte Synchronisation	Zeitpunkt der letzten Synchronisation der Azure® Active Directory® Gruppe mit dem lokalen Active Directory®.
SID der lokalen Gruppe	Sicherheits-ID (SID) der lokalen Active Directory® Gruppe.

Azure® Active Directory® Gruppe an Azure® Active Directory® Benutzerkonten zuweisen

Gruppen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Bei der indirekten Zuweisung werden Personen und Gruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die Gruppen berechnet, die einer Person zugewiesen sind.

Wenn Sie eine Person in Rollen aufnehmen und die Person ein Benutzerkonto besitzt, dann wird dieses Benutzerkonto in die Gruppen aufgenommen. Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und Gruppen erlaubt.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.

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

Detaillierte Informationen zum Thema

- [Azure® Active Directory® Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 92
- [Azure® Active Directory® Gruppe an Geschäftsrollen zuweisen](#) auf Seite 93
- [Azure® Active Directory® Benutzerkonten direkt an eine Azure® Active Directory® Gruppe zuweisen](#) auf Seite 94
- [Azure® Active Directory® Gruppe in Systemrollen aufnehmen](#) auf Seite 94
- [Azure® Active Directory® Gruppe in den IT Shop aufnehmen](#) auf Seite 95

Azure® Active Directory® Gruppe 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 die Kategorie **Azure® Active Directory® | 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.
- ODER -
- Entfernen Sie im Bereich **Zuordnungen entfernen** die Organisationen.
5. Speichern Sie die Änderungen.

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

1. Wählen Sie die Kategorie **Organisationen | Abteilungen**.
- ODER -
Wählen Sie die Kategorie **Organisationen | Kostenstellen**.
- ODER -
Wählen Sie die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **Azure® Active Directory® Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Gruppe an Geschäftsrollen zuweisen auf Seite 93](#)
- [Azure® Active Directory® Benutzerkonten direkt an eine Azure® Active Directory® Gruppe zuweisen auf Seite 94](#)
- [Azure® Active Directory® Gruppe in Systemrollen aufnehmen auf Seite 94](#)

- [Azure® Active Directory® Gruppe in den IT Shop aufnehmen auf Seite 95](#)
- [One Identity Manager Benutzer für die Verwaltung einer Azure® Active Directory®-Umgebung auf Seite 8](#)

Azure® Active Directory® Gruppe an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

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 die Kategorie **Azure® Active Directory® | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
5. Speichern Sie die Änderungen.

Um Gruppen an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **Azure® Active Directory® Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 92](#)
- [Azure® Active Directory® Benutzerkonten direkt an eine Azure® Active Directory® Gruppe zuweisen auf Seite 94](#)
- [Azure® Active Directory® Gruppe in Systemrollen aufnehmen auf Seite 94](#)
- [Azure® Active Directory® Gruppe in den IT Shop aufnehmen auf Seite 95](#)
- [One Identity Manager Benutzer für die Verwaltung einer Azure® Active Directory®-Umgebung auf Seite 8](#)

Azure® Active Directory® Benutzerkonten direkt an eine Azure® Active Directory® Gruppe zuweisen

Gruppen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der Gruppen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person ein Benutzerkonto im Azure® Active Directory®, werden die Gruppen der Rollen an dieses Benutzerkonto vererbt.

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

Um eine Gruppe direkt an Benutzerkonten zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Gruppen direkt an ein Azure® Active Directory® Benutzerkonto zuweisen auf Seite 78](#)
- [Azure® Active Directory® Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 92](#)
- [Azure® Active Directory® Gruppe an Geschäftsrollen zuweisen auf Seite 93](#)
- [Azure® Active Directory® Gruppe in Systemrollen aufnehmen auf Seite 94](#)
- [Azure® Active Directory® Gruppe in den IT Shop aufnehmen auf Seite 95](#)

Azure® Active Directory® Gruppe in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

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

- ① **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 Dell One Identity Manager Administrationshandbuch für Systemrollen.

Um eine Gruppe an Systemrollen zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | 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.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Systemrollen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 92](#)
- [Azure® Active Directory® Gruppe an Geschäftsrollen zuweisen auf Seite 93](#)
- [Azure® Active Directory® Benutzerkonten direkt an eine Azure® Active Directory® Gruppe zuweisen auf Seite 94](#)
- [Azure® Active Directory® Gruppe in den IT Shop aufnehmen auf Seite 95](#)

Azure® Active Directory® Gruppe in den IT Shop aufnehmen

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

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

① HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren Gruppen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Gruppen in den IT Shop aufzunehmen.

Um eine Gruppe in den IT Shop aufzunehmen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Gruppen** (bei nicht-rollenbasierter Anmeldung).
- ODER -
Wählen Sie die Kategorie **Berechtigungen | Azure® Active Directory® Gruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppe an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Gruppe aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Gruppen** (bei nicht-rollenbasierter Anmeldung).
- ODER -
Wählen Sie die Kategorie **Berechtigungen | Azure® Active Directory® Gruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppe aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Gruppe aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Gruppen** (bei nicht-rollenbasierter Anmeldung).
- ODER -
Wählen Sie die Kategorie **Berechtigungen | Azure® Active Directory® Gruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

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

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

Verwandte Themen

- [Allgemeine Stammdaten einer Azure® Active Directory® Gruppe auf Seite 89](#)
- [Azure® Active Directory® Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 92](#)
- [Azure® Active Directory® Gruppe an Geschäftsrollen zuweisen auf Seite 93](#)
- [Azure® Active Directory® Benutzerkonten direkt an eine Azure® Active Directory® Gruppe zuweisen auf Seite 94](#)
- [Azure® Active Directory® Gruppe in Systemrollen aufnehmen auf Seite 94](#)

Zusätzliche Aufgaben für die Verwaltung von Azure® Active Directory® Gruppen

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen

können.

Überblick über die Azure® Active Directory® Gruppe

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Gruppe.

Um einen Überblick über eine Gruppe zu erhalten

1. Wählen Sie die Kategorie **Azure® Active Directory® | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die Azure® Active Directory® Gruppe**.

Azure® Active Directory® Gruppen in Azure® Active Directory® Gruppen aufnehmen

Mit dieser Aufgabe nehmen Sie eine Gruppe in andere Gruppen auf.

Um Gruppen direkt an eine Gruppe zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Wählen Sie den Tabreiter **Hat Mitglieder**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu, die der ausgewählten Gruppe untergeordnet sind.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Wählen Sie den Tabreiter **Ist Mitglied in**.
7. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu, die der ausgewählten Gruppe übergeordnet sind.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
8. Speichern Sie die Änderungen.

Wirksamkeit von Gruppenmitgliedschaften

Tabelle 35: Konfigurationsparameter für die bedingte Vererbung

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

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

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

HINWEIS:

- Ein wechselseitiger Ausschluss zweier Gruppen kann nicht definiert werden. Das heißt, die Festlegung "Gruppe A schließt Gruppe B aus" UND "Gruppe B schließt Gruppe A aus" ist nicht zulässig.
- Für eine Gruppe muss jede auszuschließende Gruppe einzeln bekannt gegeben werden. Ausschlussdefinitionen werden nicht vererbt.
- Ob die Mitgliedschaft einer ausgeschlossenen Gruppe in einer anderen Gruppe zulässig ist, wird durch den One Identity Manager nicht überprüft.

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

Beispiel für die Wirksamkeit von Gruppenmitgliedschaften

- In einem Mandanten ist eine Gruppe A mit Berechtigungen zum Auslösen von Bestellungen definiert. Eine Gruppe B berechtigt zum Anweisen von Zahlungen. Eine Gruppe C berechtigt zum Prüfen von Rechnungen.
- Gruppe A wird über die Abteilung "Marketing", Gruppe B über die Abteilung "Finanzen" und Gruppe C wird über die Geschäftsrolle "Kontrollgruppe" zugewiesen.

Clara Harris hat ein Benutzerkonto in diesem Mandanten. Sie gehört primär der Abteilung "Marketing" an. Sekundär sind ihr die Geschäftsrolle "Kontrollgruppe" und die Abteilung "Finanzen" zugewiesen. Ohne Ausschlussdefinition erhält das Benutzerkonto alle Berechtigungen der Gruppen A, B und C.

Durch geeignete Maßnahmen soll verhindert werden, dass eine Person sowohl Bestellungen auslösen als auch Rechnungen zur Zahlung anweisen kann. Das heißt, die Gruppen A und B schließen sich aus. Eine Person, die Rechnungen prüft, darf ebenfalls keine Rechnungen zur Zahlung anweisen. Das heißt, die Gruppen B und C schließen sich aus.

Tabelle 36: Festlegen der ausgeschlossenen Gruppen (Tabelle `ADGroupExclusion`)

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

Tabelle 37: Wirksame Zuweisungen

Person	Mitglied in Rolle	Wirksame Gruppe
Ben King	Marketing	Gruppe A
Jan Bloggs	Marketing, Finanzen	Gruppe B
Clara Harris	Marketing, Finanzen, Kontrollgruppe	Gruppe C
Jenny Basset	Marketing, Kontrollgruppe	Gruppe A, Gruppe C

Für Clara Harris ist nur die Zuweisung der Gruppe C wirksam und wird ins Zielsystem publiziert. Verlässt Clara Harris die Geschäftsrolle "Kontrollgruppe" zu einem späteren Zeitpunkt, wird die Gruppe B ebenfalls wirksam.

Für Jenny Basset sind die Gruppen A und C wirksam, da zwischen beiden Gruppen kein Ausschluss definiert wurde. Das heißt, die Person ist berechtigt Bestellungen auszulösen und Rechnungen zu prüfen. Soll das verhindert werden, definieren Sie einen weiteren Ausschluss für die Gruppe C.

Tabelle 38: Ausgeschlossene Gruppen und wirksame Zuweisungen

Person	Mitglied in Rolle	Zugewiesene Gruppe	Ausgeschlossene Gruppe	Wirksame Gruppe
Jenny Basset	Marketing	Gruppe A		Gruppe C
	Kontrollgruppe	Gruppe C	Gruppe B Gruppe A	

Voraussetzungen

- Der Konfigurationsparameter „`QER\Structures\Inherit\GroupExclusion`“ ist aktiviert.
- Sich ausschließende Gruppen gehören zum selben Mandanten.

Um Gruppen auszuschließen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Gruppen**.
2. Wählen Sie in der Ergebnisliste eine Gruppe.
3. Wählen Sie die Aufgabe **Gruppen ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu, die sich mit der gewählten Gruppe ausschließen.
 - ODER -
 Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Vererbung von Azure® Active Directory® Gruppen anhand von Kategorien

Im One Identity Manager können Gruppen, Administratorrollen, Abonnements und unwirksame Dienstpläne selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen (Administratorrollen, Abonnements, unwirksame Dienstpläne) und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält verschiedene Tabellen. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In den übrigen Tabellen geben Sie Ihre Kategorien für die zielsystemabhängigen Gruppen, Administratorrollen, Abonnements und unwirksamen Dienstpläne an. Jede Tabelle enthält die Kategoriepositionen „Position1“ bis „Position 31“.

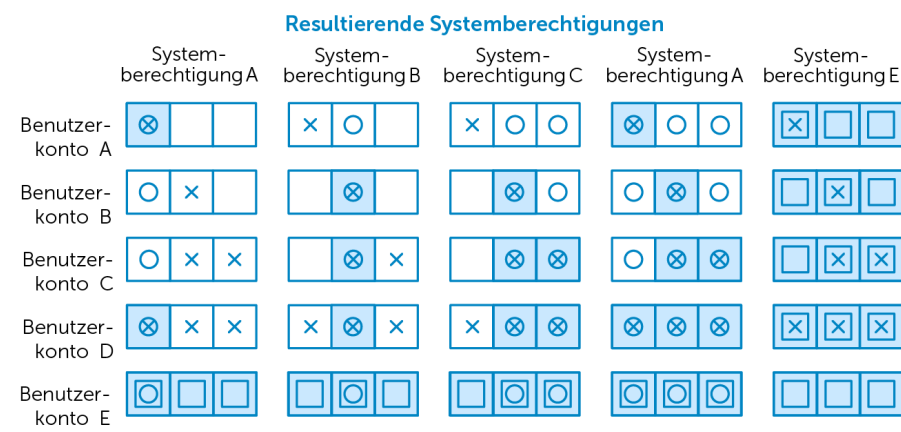
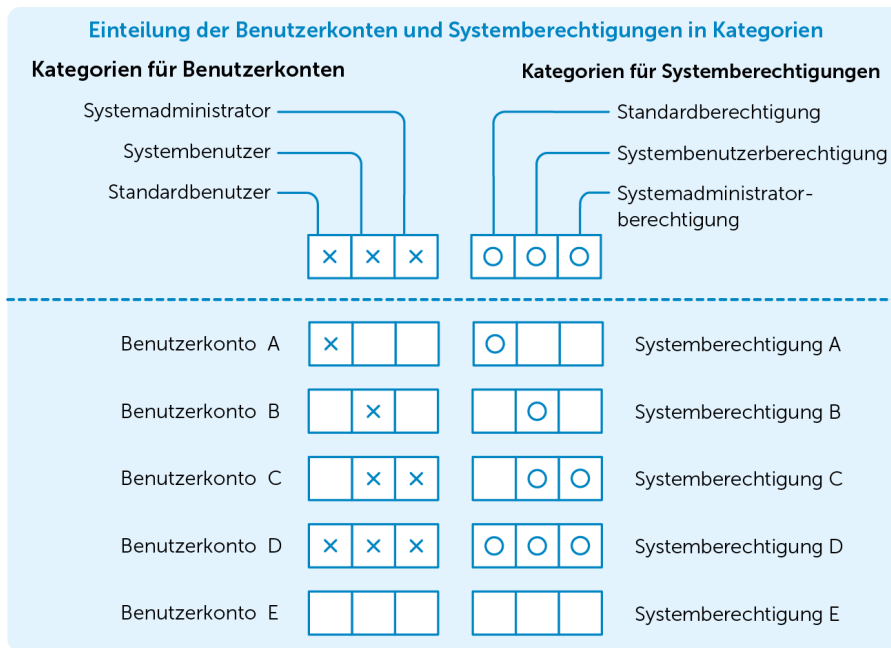
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto vererbt. Ist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

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


Tabelle 39: Beispiele für Kategorien

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

Abbildung 2: Beispiel für die Vererbung über Kategorien



Legende:

-  Vererbt aufgrund passender Kategorien
-  Vererbt, da das Benutzerkonto nicht kategorisiert ist
-  Vererbt, da Benutzerkonto und Systemberechtigung nicht kategorisiert sind
-  Vererbt, da die Systemberechtigung nicht kategorisiert ist

Um die Vererbung über Kategorien zu nutzen

- Definieren Sie am Mandanten die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Gruppen über ihre Stammdaten zu.

Verwandte Themen

- [Festlegen der Kategorien für die Vererbung von Berechtigungen auf Seite 63](#)
- [Allgemeine Stammdaten eines Azure® Active Directory® Benutzerkontos auf Seite 72](#)

- [Allgemeine Stammdaten einer Azure® Active Directory® Gruppe](#) auf Seite 89
- Weitere Informationen finden Sie unter [Bearbeiten der Stammdaten von Azure® Active Directory® Abonnements](#) auf Seite 113.

Eigentümer an Azure® Active Directory® Gruppen zuweisen

Die Eigentümer einer Gruppen können die Eigenschaften einer Gruppe bearbeiten.

Um Eigentümer an eine Gruppe zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste **Tabelle** die Tabelle, welche die Eigentümer enthält. Zur Auswahl stehen:
 - Azure® Active Directory® Benutzerkonten
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Eigentümer zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Eigentümer.
6. Speichern Sie die Änderungen.

Zusatzeigenschaften an eine Azure® Active Directory® Gruppe zuweisen

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

Um Zusatzeigenschaften für eine Gruppe festzulegen


1. Wählen Sie die Kategorie **Azure® Active Directory® | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Zusatzeigenschaften.
5. Speichern Sie die Änderungen.

Verwandte Themen

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

Löschen von Azure® Active Directory® Gruppen

Um eine Gruppe zu löschen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Löschen Sie die Gruppe über die Schaltfläche .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Die Gruppe wird endgültig aus der One Identity Manager-Datenbank und der Azure® Active Directory®-Umgebung gelöscht.

Azure® Active Directory® Administratorrollen

Mithilfe von Administratorrollen können Sie Benutzern administrative Berechtigungen zuweisen. Azure® Active Directory® kennt verschiedene Administratorrollen, die unterschiedliche Funktionen erfüllen. Ausführliche Informationen zu Administratorrollen finden Sie in der Azure® Active Directory® Dokumentation von Microsoft.

Administratorrollen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können einzelne Stammdaten der Administratorrollen bearbeiten. Neue Administratorrollen können Sie im One Identity Manager nicht erstellen.

Um Benutzer in Administratorrollen aufzunehmen, können Sie die Administratorrollen direkt an die Benutzer zuweisen. Sie können Administratorrollen an Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder den IT Shop zuweisen.

Bearbeiten der Stammdaten einer Azure® Active Directory® Administratorrolle

Administratorrollen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können einzelne Stammdaten der Administratorrollen bearbeiten. Neue Administratorrollen können Sie im One Identity Manager nicht erstellen.

Um die Stammdaten einer Administratorrolle zu bearbeiten

1. Wählen Sie die Kategorie **Azure® Active Directory® | Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten für eine Administratorrolle.
4. Speichern Sie die Änderungen.

Tabelle 40: Stammdaten einer Administratorrolle

Eigenschaft	Beschreibung
Anzeigename	Anzeigename zur Anzeige der Administratorrolle in der Benutzeroberfläche der One Identity Manager Werkzeuge.
Mandant	Mandant der Administratorrolle.
ID der Vorlage	ID der Administratorrollenvorlage auf der diese Administratorrolle basiert.
IT Shop	Angabe, ob die Administratorrolle über den IT Shop bestellbar ist. Die Administratorrolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Administratorrolle kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Administratorrolle ausschließlich über den IT Shop bestellbar ist. Die Administratorrolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Administratorrolle an hierarchische Rollen ist nicht zulässig.
Leistungsposition	Angabe einer Leistungsposition, um die Administratorrolle über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Administratorrolle an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter „QER\CalculateRiskIndex“ aktiviert ist.
Kategorie	Kategorien für die Vererbung von Administratorrolle. Administratorrollen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Administratorrollen und die Benutzerkonten in Kategorien eingeteilt. Über die Auswahlliste ordnen Sie die Administratorrolle einer oder mehreren Kategorien zu.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Verwandte Themen

- [Vererbung von Azure® Active Directory® Administratorrollen anhand von Kategorien auf Seite 112](#)
- Ausführliche Informationen zur Risikobewertung finden Sie im Dell One Identity Manager Administrationshandbuch für Risikobewertungen.
- Ausführliche Informationen zur Vorbereitung der Gruppen für die Bestellung über den IT Shop finden Sie im Dell One Identity Manager Administrationshandbuch für IT Shop.

Azure® Active Directory® Administratorrollen an Azure® Active Directory® Benutzerkonten zuweisen

Administratorrollen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Bei der indirekten Zuweisung werden Personen und Administratorrollen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die Administratorrollen berechnet, die einer Person zugewiesen sind.

Wenn Sie eine Person in Rollen aufnehmen und die Person ein Benutzerkonto besitzt, dann wird dieses Benutzerkonto in die Administratorrollen aufgenommen. Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und Administratorrollen erlaubt.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.

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

Detaillierte Informationen zum Thema

- [Azure® Active Directory® Administratorrolle an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 106](#)
- [Azure® Active Directory® Administratorrolle an Geschäftsrollen zuweisen auf Seite 107](#)
- [Azure® Active Directory® Benutzerkonten direkt an eine Azure® Active Directory® Administratorrolle zuweisen auf Seite 108](#)
- [Azure® Active Directory® Administratorrolle in Systemrollen aufnehmen auf Seite 109](#)
- [Azure® Active Directory® Administratorrolle in den IT Shop aufnehmen auf Seite 110](#)

Azure® Active Directory® Administratorrolle an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Administratorrolle an Abteilungen, Kostenstellen oder Standorte zu, damit die Administratorrolle über diese Organisationen an Benutzerkonten zugewiesen wird.

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

1. Wählen Sie die Kategorie **Azure® Active Directory® | Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
 - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
 - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
 - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

- ODER -

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

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

1. Wählen Sie die Kategorie **Organisationen | Abteilungen**.
- ODER -
Wählen Sie die Kategorie **Organisationen | Kostenstellen**.
- ODER -
Wählen Sie die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **Azure® Active Directory® Administratorrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Administratorrollen zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Administratorrollen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Administratorrolle an Geschäftsrollen zuweisen auf Seite 107](#)
- [Azure® Active Directory® Benutzerkonten direkt an eine Azure® Active Directory® Administratorrolle zuweisen auf Seite 108](#)
- [Azure® Active Directory® Administratorrolle in Systemrollen aufnehmen auf Seite 109](#)
- [Azure® Active Directory® Administratorrolle in den IT Shop aufnehmen auf Seite 110](#)
- [One Identity Manager Benutzer für die Verwaltung einer Azure® Active Directory®-Umgebung auf Seite 8](#)

Azure® Active Directory® Administratorrolle an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie die Administratorrolle an Geschäftsrollen zu, damit die Administratorrolle über diese Geschäftsrollen an Benutzerkonten zugewiesen wird.

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

1. Wählen Sie die Kategorie **Azure® Active Directory® | Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
5. Speichern Sie die Änderungen.

Um Administratorrollen an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **Geschäftsrollen** | **<Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **Azure® Active Directory® Administratorrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Administratorrollen zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Administratorrollen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Administratorrolle an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 106](#)
- [Azure® Active Directory® Benutzerkonten direkt an eine Azure® Active Directory® Administratorrolle zuweisen auf Seite 108](#)
- [Azure® Active Directory® Administratorrolle in Systemrollen aufnehmen auf Seite 109](#)
- [Azure® Active Directory® Administratorrolle in den IT Shop aufnehmen auf Seite 110](#)
- [One Identity Manager Benutzer für die Verwaltung einer Azure® Active Directory®-Umgebung auf Seite 8](#)

Azure® Active Directory® Benutzerkonten direkt an eine Azure® Active Directory® Administratorrolle zuweisen

Administratorrollen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der Administratorrollen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person ein Benutzerkonto im Azure® Active Directory®, werden die Administratorrollen der Rollen an dieses Benutzerkonto vererbt.

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

Um eine Administratorrolle direkt an Benutzerkonten zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory®** | **Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Administratorrollen direkt an ein Azure® Active Directory® Benutzerkonto zuweisen auf Seite 78](#)
- [Azure® Active Directory® Administratorrolle an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 106](#)
- [Azure® Active Directory® Administratorrolle an Geschäftsrollen zuweisen auf Seite 107](#)
- [Azure® Active Directory® Administratorrolle in Systemrollen aufnehmen auf Seite 109](#)
- [Azure® Active Directory® Administratorrolle in den IT Shop aufnehmen auf Seite 110](#)

Azure® Active Directory® Administratorrolle in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

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

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

Um eine Administratorrolle an Systemrollen zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Systemrollen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Administratorrolle an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 106](#)
- [Azure® Active Directory® Administratorrolle an Geschäftsrollen zuweisen auf Seite 107](#)
- [Azure® Active Directory® Benutzerkonten direkt an eine Azure® Active Directory® Administratorrolle zuweisen auf Seite 108](#)
- [Azure® Active Directory® Administratorrolle in den IT Shop aufnehmen auf Seite 110](#)

Azure® Active Directory® Administratorrolle in den IT Shop aufnehmen

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

- Die Administratorrolle muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Administratorrolle muss eine Leistungsposition zugeordnet sein.
- Soll die Administratorrolle nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss die Administratorrolle 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 Administratorrollen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Administratorrollen in den IT Shop aufzunehmen.

Um eine Administratorrolle in den IT Shop aufzunehmen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Administratorrollen** (bei nicht-rollenbasierter Anmeldung).
- ODER -
Wählen Sie die Kategorie **Berechtigungen | Azure® Active Directory® Administratorrollen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Administratorrolle an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Administratorrolle aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Administratorrollen** (bei nicht-rollenbasierter Anmeldung).
- ODER -
Wählen Sie die Kategorie **Berechtigungen | Azure® Active Directory® Administratorrollen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Administratorrolle aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Administratorrolle aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Administratorrollen** (bei nicht-rollenbasierter Anmeldung).
- ODER -

Wählen Sie die Kategorie **Berechtigungen | Azure® Active Directory® Administratorrollen** (bei rollenbasierter Anmeldung).

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

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

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

Verwandte Themen

- [Bearbeiten der Stammdaten einer Azure® Active Directory® Administratorrolle auf Seite 104](#)
- [Azure® Active Directory® Administratorrolle an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 106](#)
- [Azure® Active Directory® Administratorrolle an Geschäftsrollen zuweisen auf Seite 107](#)
- [Azure® Active Directory® Benutzerkonten direkt an eine Azure® Active Directory® Administratorrolle zuweisen auf Seite 108](#)
- [Azure® Active Directory® Administratorrolle in Systemrollen aufnehmen auf Seite 109](#)

Zusätzliche Aufgaben für die Verwaltung von Azure® Active Directory® Administratorrollen

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können.

Überblick über die Azure® Active Directory® Administratorrolle

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Administratorrolle.

Um einen Überblick über eine Administratorrolle zu erhalten

1. Wählen Sie die Kategorie **Azure® Active Directory® | Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **Überblick über die Azure® Active Directory® Administratorrolle**.

Vererbung von Azure® Active Directory® Administratorrollen anhand von Kategorien

Das unter [Vererbung von Azure® Active Directory® Gruppen anhand von Kategorien](#) auf Seite 100 beschriebene Verhalten können Sie auch für Administratorrollen einsetzen.

Um die Vererbung über Kategorien zu nutzen

- Definieren Sie am Mandanten die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Administratorrollen über ihre Stammdaten zu.

Verwandte Themen

- [Festlegen der Kategorien für die Vererbung von Berechtigungen](#) auf Seite 63
- [Allgemeine Stammdaten eines Azure® Active Directory® Benutzerkontos](#) auf Seite 72
- [Bearbeiten der Stammdaten einer Azure® Active Directory® Administratorrolle](#) auf Seite 104

Zusatzeigenschaften an eine Azure® Active Directory® Administratorrolle zuweisen

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

Um Zusatzeigenschaften für eine Administratorrolle festzulegen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Zusatzeigenschaften.
5. Speichern Sie die Änderungen.

Verwandte Themen

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

Azure® Active Directory® Abonnements und Dienstpläne

Um auf die Dienstpläne im Azure® Active Directory® zuzugreifen, benötigen die Benutzer ein Abonnement. Ein Benutzer erhält alle Dienstpläne, die mit einem Abonnement verknüpft sind. Um den Benutzern Abonnements zur Verfügung zu stellen, können Sie die Abonnements direkt an die Benutzer zuweisen. Sie können Abonnements an Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder den IT Shop zuweisen.

Um für die Benutzer die Nutzung einzelner Dienstpläne zu unterbinden, werden im One Identity Manager zusätzlich sogenannte "unwirksame Dienstpläne" abgebildet. Unwirksame Dienstpläne werden nach der Synchronisation der Abonnements automatisch im One Identity Manager erzeugt. Unwirksame Dienstpläne werden über den IT Shop bestellt oder über Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder Systemrollen den Benutzern zugewiesen.

Aus den Abonnements eines Benutzers mit den damit verbundenen Dienstplänen und der Zuweisung unwirksamer Dienstpläne ergeben sich die tatsächlich für den Benutzer im Azure® Active Directory® verfügbaren Dienstpläne.

Azure® Active Directory® Abonnements

Die Informationen zu Abonnements und Dienstplänen innerhalb eines Mandanten werden durch die Synchronisation in den One Identity Manager eingelesen. Neue Abonnements und Dienstpläne können Sie im One Identity Manager nicht erstellen. Sie können im One Identity Manager einzelne Stammdaten der Abonnements für die Bestellung im IT Shop und die Zuweisung an Benutzerkonten bearbeiten.

Bearbeiten der Stammdaten von Azure® Active Directory® Abonnements

Um die Stammdaten eines Abonnements zu bearbeiten

1. Wählen Sie die Kategorie **Azure® Active Directory® | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Abonnements.
5. Speichern Sie die Änderungen.

Tabelle 41: Stammdaten eines Abonnements

Eigenschaft	Beschreibung
SKU Anzeigename	SKU Anzeigename des Abonnements, beispielsweise "AAD_Premium" oder "RMSBASIC".
Mandant	Mandant, zu dem dieses Abonnement eingetragen ist.
Abonnementstatus	Angabe des Status des Abonnements, beispielsweise "enabled" (aktiv).
Gekaufte Lizenzen	Anzahl der gekauften Lizenzen.
Zugewiesene Lizenzen	Anzahl der aktiv genutzten Lizenzen.
Gesperrte Lizenzen	Anzahl der gesperrten Lizenzen.
Warnungseinheiten	Anzahl der Lizenzen, die im Warnungsstatus sind.
IT Shop	Angabe, ob das Abonnement über den IT Shop bestellbar ist. Das Abonnement kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Das Abonnement kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob das Abonnement ausschließlich über den IT Shop bestellbar ist. Das Abonnement kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung des Abonnements an hierarchische Rollen ist nicht zulässig.
Leistungsposition	Angabe einer Leistungsposition, um das Abonnement über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen des Abonnements an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter „QER\CalculateRiskIndex“ aktiviert ist.
Kategorie	Kategorien für die Vererbung von Abonnements. Abonnements können selektiv an Benutzerkonten vererbt werden. Dazu werden die Abonnements und die Benutzerkonten in Kategorien eingeteilt. Über die Auswahlliste ordnen Sie das Abonnement einer oder mehreren Kategorien zu.

Verwandte Themen

- [Vererbung von Azure® Active Directory® Gruppen anhand von Kategorien](#) auf Seite 100
- Ausführliche Informationen zur Risikobewertung finden Sie im Dell One Identity Manager Administrationshandbuch für Risikobewertungen.
- Ausführliche Informationen zur Vorbereitung der Gruppen für die Bestellung über den IT Shop finden Sie im Dell One Identity Manager Administrationshandbuch für IT Shop.

Azure® Active Directory® Abonnements an Azure® Active Directory® Benutzerkonten zuweisen

Abonnements können Sie einem Benutzerkonto direkt oder indirekt zuweisen. Bei der indirekten Zuweisung werden Personen und Abonnements in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die Abonnements berechnet, die einer Person zugewiesen sind.

Besitzt die Person ein Benutzerkonto im Azure® Active Directory®, werden die Abonnements der Rollen an dieses Benutzerkonto vererbt.

Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und Abonnements erlaubt.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.

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

TIPP: Damit eine Person automatisiert ein Benutzerkonto und ein Abonnement erhält, können Sie die Kontendefinition zur Erstellung des Benutzerkontos und das zu verwendende Abonnement in einer Systemrolle zusammenfassen.

Eine Person kann diese Systemrolle direkt erhalten, über Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen erben oder über den IT Shop bestellen.

Detaillierte Informationen zum Thema

- [Azure® Active Directory® Abonnement an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 115](#)
- [Azure® Active Directory® Abonnement an Geschäftsrollen zuweisen auf Seite 117](#)
- [Azure® Active Directory® Benutzerkonten direkt an ein Azure® Active Directory® Abonnement zuweisen auf Seite 117](#)
- [Azure® Active Directory® Abonnement in Systemrollen aufnehmen auf Seite 118](#)
- [Azure® Active Directory® Abonnement in den IT Shop aufnehmen auf Seite 119](#)

Azure® Active Directory® Abonnement an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Abonnements an Abteilungen, Kostenstellen oder Standorte zu, damit sie über diese Organisationen an Benutzerkonten zugewiesen wird.

Um ein Abonnement an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **Azure® Active Directory® | Abonnements**.
 2. Wählen Sie in der Ergebnisliste das Abonnement.
 3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
 4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
 - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
 - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
 - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.
- ODER -
- Entfernen Sie im Bereich **Zuordnungen entfernen** die Organisationen.
5. Speichern Sie die Änderungen.

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

1. Wählen Sie die Kategorie **Organisationen | Abteilungen**.
- ODER -
Wählen Sie die Kategorie **Organisationen | Kostenstellen**.
- ODER -
Wählen Sie die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **Azure® Active Directory® Abonnement zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Abonnements zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Abonnements.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Abonnement an Geschäftsrollen zuweisen auf Seite 117](#)
- [Azure® Active Directory® Benutzerkonten direkt an ein Azure® Active Directory® Abonnement zuweisen auf Seite 117](#)
- [Azure® Active Directory® Abonnement in Systemrollen aufnehmen auf Seite 118](#)
- [Azure® Active Directory® Abonnement in den IT Shop aufnehmen auf Seite 119](#)
- [One Identity Manager Benutzer für die Verwaltung einer Azure® Active Directory®-Umgebung auf Seite 8](#)

Azure® Active Directory® Abonnement an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie die Abonnements an Geschäftsrollen zu, damit die sie über diese Geschäftsrollen an Benutzerkonten zugewiesen wird.

Um ein Abonnement an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **Azure® Active Directory® | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
5. Speichern Sie die Änderungen.

Um Abonnements an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **Azure® Active Directory® Abonnements zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Abonnements zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Abonnements.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Abonnement an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 115](#)
- [Azure® Active Directory® Benutzerkonten direkt an ein Azure® Active Directory® Abonnement zuweisen auf Seite 117](#)
- [Azure® Active Directory® Abonnement in Systemrollen aufnehmen auf Seite 118](#)
- [Azure® Active Directory® Abonnement in den IT Shop aufnehmen auf Seite 119](#)
- [One Identity Manager Benutzer für die Verwaltung einer Azure® Active Directory®-Umgebung auf Seite 8](#)

Azure® Active Directory® Benutzerkonten direkt an ein Azure® Active Directory® Abonnement zuweisen

Abonnements können Sie einem Benutzerkonto direkt oder indirekt zuweisen. Bei der indirekten Zuweisung werden Personen und Abonnements in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder

Geschäftsrollen eingeordnet. Besitzt die Person ein Benutzerkonto im Azure® Active Directory®, werden die Abonnements der Rollen an dieses Benutzerkonto vererbt.

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

Um ein Abonnement direkt an Benutzerkonten zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Abonnements direkt an Azure® Active Directory® Benutzerkonten zuweisen auf Seite 79](#)
- [Azure® Active Directory® Abonnement an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 115](#)
- [Azure® Active Directory® Abonnement an Geschäftsrollen zuweisen auf Seite 117](#)
- [Azure® Active Directory® Abonnement in Systemrollen aufnehmen auf Seite 118](#)
- [Azure® Active Directory® Abonnement in den IT Shop aufnehmen auf Seite 119](#)

Azure® Active Directory® Abonnement in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

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

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

Um ein Abonnement an Systemrollen zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.
- ODER -

Entfernen Sie im Bereich **Zuordnungen entfernen** die Systemrollen.

5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Abonnement an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 115](#)
- [Azure® Active Directory® Abonnement an Geschäftsrollen zuweisen auf Seite 117](#)
- [Azure® Active Directory® Benutzerkonten direkt an ein Azure® Active Directory® Abonnement zuweisen auf Seite 117](#)
- [Azure® Active Directory® Abonnement in den IT Shop aufnehmen auf Seite 119](#)

Azure® Active Directory® Abonnement in den IT Shop aufnehmen

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

- Das Abonnement muss mit der Option **IT Shop** gekennzeichnet sein.
- Dem Abonnement muss eine Leistungsposition zugeordnet sein.
- Soll das Abonnement nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss das Abonnement 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 Abonnements an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Abonnements in den IT Shop aufzunehmen.

Um ein Abonnement in den IT Shop aufzunehmen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Abonnements** (bei nicht-rollenbasierter Anmeldung).
- ODER -
Wählen Sie die Kategorie **Berechtigungen | Azure® Active Directory® Abonnements** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** das Abonnement an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um ein Abonnement aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Abonnements** (bei nicht-rollenbasierter Anmeldung).
- ODER -

Wählen Sie die Kategorie **Berechtigungen | Azure® Active Directory® Abonnements** (bei rollenbasierter Anmeldung).

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

Um ein Abonnement aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Abonnements** (bei nicht-rollenbasierter Anmeldung).

- ODER -

Wählen Sie die Kategorie **Berechtigungen | Azure® Active Directory® Abonnements** (bei rollenbasierter Anmeldung).

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

Das Abonnement wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen dieses Abonnements abbestellt.

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

Verwandte Themen

- [Bearbeiten der Stammdaten von Azure® Active Directory® Abonnements auf Seite 113](#)
- [Azure® Active Directory® Abonnement an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 115](#)
- [Azure® Active Directory® Abonnement an Geschäftsrollen zuweisen auf Seite 117](#)
- [Azure® Active Directory® Benutzerkonten direkt an ein Azure® Active Directory® Abonnement zuweisen auf Seite 117](#)
- [Azure® Active Directory® Abonnement in Systemrollen aufnehmen auf Seite 118](#)

Zusätzliche Aufgaben für die Verwaltung von Azure® Active Directory® Abonnements

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können.

Überblick über Azure® Active Directory® Abonnements

Um einen Überblick über ein Abonnement zu erhalten

1. Wählen Sie die Kategorie **Azure® Active Directory® | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Überblick über das Azure® Active Directory® Abonnement**.

Um einen Überblick über einen Dienstplan zu erhalten

1. Wählen Sie die Kategorie **Azure® Active Directory® | Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Überblick über den Azure® Active Directory® Dienstplan**.

Um einen Überblick über einen unwirksamen Dienstpläne zu erhalten

1. Wählen Sie die Kategorie **Azure® Active Directory® | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Überblick über den unwirksamen Azure® Active Directory® Dienstplan**.

Wirksamkeit von Abonnementzuweisungen

Das unter [Wirksamkeit von Gruppenmitgliedschaften](#) auf Seite 98 beschriebene Verhalten können Sie auch für Abonnements einsetzen. Die Wirksamkeit der Zuweisungen wird in den Tabellen `AADUserHasSubSku` und `AADBaseTreeHasSubSku` über die Spalte `XIsInEffect` abgebildet.

Voraussetzungen

- Der Konfigurationsparameter „`QER\Structures\Inherit\GroupExclusion`“ ist aktiviert.
- Sich ausschließende Abonnements gehören zum selben Mandanten.

Um Abonnements auszuschließen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Abonnements ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Abonnements zu, die sich mit dem gewählten Abonnement ausschließen.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Abonnements, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Vererbung von Azure® Active Directory® Abonnements anhand von Kategorien

Das unter [Vererbung von Azure® Active Directory® Gruppen anhand von Kategorien](#) auf Seite 100 beschriebene Verhalten können Sie auch für Abonnements einsetzen.

Um die Vererbung über Kategorien zu nutzen

- Definieren Sie am Mandanten die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Abonnements über ihre Stammdaten zu.

Verwandte Themen

- [Festlegen der Kategorien für die Vererbung von Berechtigungen](#) auf Seite 63
- [Allgemeine Stammdaten eines Azure® Active Directory® Benutzerkontos](#) auf Seite 72
- [Bearbeiten der Stammdaten von Azure® Active Directory® Abonnements](#) auf Seite 113

Zusatzeigenschaften an ein Azure® Active Directory® Abonnement zuweisen

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

Um Zusatzeigenschaften für ein Abonnement festzulegen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Zusatzeigenschaften.
5. Speichern Sie die Änderungen.

Verwandte Themen

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

Unwirksame Azure® Active Directory® Dienstpläne

Um für die Benutzer die Nutzung einzelner Dienstpläne zu unterbinden, werden im One Identity Manager zusätzlich sogenannte "unwirksame Dienstpläne" abgebildet. Unwirksame Dienstpläne werden nach der

Synchronisation der Abonnements automatisch im One Identity Manager erzeugt. Unwirksame Dienstpläne werden über den IT Shop bestellt oder über Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder Systemrollen den Benutzern zugewiesen.

Bearbeiten der Stammdaten von unwirksamen Azure® Active Directory® Dienstplänen

Um die Stammdaten eines unwirksamen Dienstplans zu bearbeiten

1. Wählen Sie die Kategorie **Azure® Active Directory® | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Dienstplans.
5. Speichern Sie die Änderungen.

Tabelle 42: Stammdaten eines unwirksamen Dienstplans

Eigenschaft	Beschreibung
Abonnement	Bezeichnung des Abonnements.
Dienstplan	Bezeichnung des Dienstplans.
IT Shop	Angabe, ob der unwirksame Dienstplan über den IT Shop bestellbar ist. Der unwirksame Dienstplan kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Der unwirksame Dienstplan kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob der unwirksame Dienstplan ausschließlich über den IT Shop bestellbar ist. Der unwirksame Dienstplan kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung des unwirksamen Dienstplans an hierarchische Rollen ist nicht zulässig.
Leistungsposition	Angabe einer Leistungsposition, um den unwirksamen Dienstplan über den IT Shop zu bestellen.
Kategorie	Kategorien für die Vererbung von unwirksamen Dienstpläne. Unwirksame Dienstpläne können selektiv an Benutzerkonten vererbt werden. Dazu werden die unwirksamen Dienstpläne und die Benutzerkonten in Kategorien eingeteilt. Über die Auswahlliste ordnen Sie den unwirksamen Dienstplan einer oder mehreren Kategorien zu.

Verwandte Themen

- [Vererbung von Azure® Active Directory® Gruppen anhand von Kategorien](#) auf Seite 100
- Ausführliche Informationen zur Vorbereitung der Gruppen für die Bestellung über den IT Shop finden Sie im Dell One Identity Manager Administrationshandbuch für IT Shop.

Unwirksame Azure® Active Directory® Dienstpläne an Azure® Active Directory® Benutzerkonten zuweisen

Unwirksame Dienstpläne können Sie einem Benutzerkonto direkt oder indirekt zuweisen. Bei der indirekten Zuweisung werden Personen und unwirksame Dienstpläne in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die unwirksamen Dienstplänen berechnet, die einer Person zugewiesen sind.

Besitzt die Person ein Benutzerkonto im Azure® Active Directory®, werden die unwirksamen Dienstpläne der Rollen an dieses Benutzerkonto vererbt.

Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und unwirksame Dienstpläne erlaubt.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.

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

Detaillierte Informationen zum Thema

- [Unwirksamen Azure® Active Directory® Dienstplan an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 124
- [Unwirksamen Azure® Active Directory® Dienstplan an Geschäftsrollen zuweisen](#) auf Seite 125
- [Azure® Active Directory® Benutzerkonten direkt an unwirksamen Azure® Active Directory® Dienstplan zuweisen](#) auf Seite 126
- [Unwirksamen Azure® Active Directory® Dienstplan in Systemrollen aufnehmen](#) auf Seite 127
- [Unwirksamen Azure® Active Directory® Dienstplan in den IT Shop aufnehmen](#) auf Seite 128

Unwirksamen Azure® Active Directory® Dienstplan an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die unwirksamen Dienstpläne an Abteilungen, Kostenstellen oder Standorte zu, damit sie über diese Organisationen an Benutzerkonten zugewiesen wird.

Um einen unwirksamen Dienstplan an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **Azure® Active Directory® | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.

- Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
- Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
- Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

- ODER -

Entfernen Sie im Bereich **Zuordnungen entfernen** die Organisationen.

5. Speichern Sie die Änderungen.

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

1. Wählen Sie die Kategorie **Organisationen | Abteilungen**.

- ODER -

Wählen Sie die Kategorie **Organisationen | Kostenstellen**.

- ODER -

Wählen Sie die Kategorie **Organisationen | Standorte**.

2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **Unwirksamen Azure® Active Directory® Dienstplan zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Dienstpläne zu.

- ODER -

Entfernen Sie im Bereich **Zuordnungen entfernen** die Dienstpläne.

5. Speichern Sie die Änderungen.

Verwandte Themen

- [Unwirksamen Azure® Active Directory® Dienstplan an Geschäftsrollen zuweisen auf Seite 125](#)
- [Azure® Active Directory® Benutzerkonten direkt an unwirksamen Azure® Active Directory® Dienstplan zuweisen auf Seite 126](#)
- [Unwirksamen Azure® Active Directory® Dienstplan in Systemrollen aufnehmen auf Seite 127](#)
- [Unwirksamen Azure® Active Directory® Dienstplan in den IT Shop aufnehmen auf Seite 128](#)
- [One Identity Manager Benutzer für die Verwaltung einer Azure® Active Directory®-Umgebung auf Seite 8](#)

Unwirksamen Azure® Active Directory® Dienstplan an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie die unwirksamen Dienstpläne an Geschäftsrollen zu, damit die sie über diese Geschäftsrollen an Benutzerkonten zugewiesen wird.

Um einen unwirksamen Dienstplan an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **Azure® Active Directory® | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
5. Speichern Sie die Änderungen.

Um unwirksame Dienstpläne an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **Unwirksamen Azure® Active Directory® Dienstplan zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Dienstpläne zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Dienstpläne.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Unwirksamen Azure® Active Directory® Dienstplan an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 124](#)
- [Azure® Active Directory® Benutzerkonten direkt an unwirksamen Azure® Active Directory® Dienstplan zuweisen auf Seite 126](#)
- [Unwirksamen Azure® Active Directory® Dienstplan in Systemrollen aufnehmen auf Seite 127](#)
- [Unwirksamen Azure® Active Directory® Dienstplan in den IT Shop aufnehmen auf Seite 128](#)
- [One Identity Manager Benutzer für die Verwaltung einer Azure® Active Directory®-Umgebung auf Seite 8](#)

Azure® Active Directory® Benutzerkonten direkt an unwirksamen Azure® Active Directory® Dienstplan zuweisen

Unwirksame Dienstpläne können Sie einem Benutzerkonto direkt oder indirekt zuweisen. Bei der indirekten Zuweisung werden Personen und unwirksame Dienstpläne in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Besitzt die Person ein Benutzerkonto im Azure® Active Directory®, werden die unwirksamen Dienstpläne der Rollen an dieses Benutzerkonto vererbt.

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

Um einen unwirksamen Dienstplan direkt an Benutzerkonten zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Azure® Active Directory® Abonnements direkt an Azure® Active Directory® Benutzerkonten zuweisen auf Seite 79](#)
- [Unwirksamen Azure® Active Directory® Dienstplan an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 124](#)
- [Unwirksamen Azure® Active Directory® Dienstplan an Geschäftsrollen zuweisen auf Seite 125](#)
- [Unwirksamen Azure® Active Directory® Dienstplan in Systemrollen aufnehmen auf Seite 127](#)
- [Unwirksamen Azure® Active Directory® Dienstplan in den IT Shop aufnehmen auf Seite 128](#)

Unwirksamen Azure® Active Directory® Dienstplan in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

Mit dieser Aufgabe nehmen Sie einen unwirksamen Dienstplan in Systemrollen auf. Wenn Sie eine Systemrolle an Personen zuweisen, wird der unwirksame Dienstplan an alle Benutzerkonten vererbt, die diese Personen besitzen.

- ① **HINWEIS:** Unwirksame Dienstpläne, bei denen die Option **Verwendung nur im IT Shop aktiviert** ist, können nur an Systemrollen zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist. Weitere Informationen finden Sie im Dell One Identity Manager Administrationshandbuch für Systemrollen.

Um einen unwirksamen Dienstplan an Systemrollen zuzuweisen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Systemrollen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Unwirksamen Azure® Active Directory® Dienstplan an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 124](#)
- [Unwirksamen Azure® Active Directory® Dienstplan an Geschäftsrollen zuweisen auf Seite 125](#)
- [Azure® Active Directory® Benutzerkonten direkt an unwirksamen Azure® Active Directory® Dienstplan zuweisen auf Seite 126](#)
- [Unwirksamen Azure® Active Directory® Dienstplan in den IT Shop aufnehmen auf Seite 128](#)

Unwirksamen Azure® Active Directory® Dienstplan in den IT Shop aufnehmen

Mit der Zuweisung eines unwirksamen Dienstplans an ein IT Shop Regal kann dieser von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Der unwirksame Dienstplan muss mit der Option **IT Shop** gekennzeichnet sein.
- Dem unwirksamen Dienstplan muss eine Leistungsposition zugeordnet sein.
- Soll der unwirksame Dienstplan nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss der Dienstplan 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 unwirksame Dienstpläne an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt unwirksame Dienstpläne in den IT Shop aufzunehmen.

Um einen unwirksamen Dienstplan in den IT Shop aufzunehmen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Unwirksame Dienstpläne** (bei nicht-rollenbasierter Anmeldung).
- ODER -
Wählen Sie die Kategorie **Berechtigungen | Unwirksame Azure® Active Directory® Dienstpläne** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** den Dienstplan an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um einen unwirksamen Dienstplan aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Unwirksame Dienstpläne** (bei nicht-rollenbasierter Anmeldung).
- ODER -
Wählen Sie die Kategorie **Berechtigungen | Unwirksame Azure® Active Directory® Dienstpläne** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.

4. Entfernen Sie im Bereich **Zuordnungen entfernen** den Dienstplan aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um einen unwirksamen Dienstplan aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Unwirksame Dienstpläne** (bei nicht-rollebasierter Anmeldung).
- ODER -
Wählen Sie die Kategorie **Berechtigungen | Unwirksame Azure® Active Directory® Dienstpläne** (bei rollebasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

Der unwirksame Dienstplan wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen dieses unwirksamen Dienstplans abbestellt.

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

Verwandte Themen

- [Unwirksamen Azure® Active Directory® Dienstplan an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 124](#)
- [Unwirksamen Azure® Active Directory® Dienstplan an Geschäftsrollen zuweisen auf Seite 125](#)
- [Azure® Active Directory® Benutzerkonten direkt an unwirksamen Azure® Active Directory® Dienstplan zuweisen auf Seite 126](#)
- [Unwirksamen Azure® Active Directory® Dienstplan in Systemrollen aufnehmen auf Seite 127](#)

Zusätzliche Aufgaben für die Verwaltung von unwirksamen Azure® Active Directory® Dienstplänen

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können.

Überblick über unwirksamen Azure® Active Directory® Dienstpläne

Um einen Überblick über einen unwirksamen Dienstpläne zu erhalten

1. Wählen Sie die Kategorie **Azure® Active Directory® | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Überblick über den unwirksamen Azure® Active Directory® Dienstplan**.

Wirksamkeit von Zuweisungen unwirksamer Dienstpläne

Das unter [Wirksamkeit von Gruppenmitgliedschaften](#) auf Seite 98 beschriebene Verhalten können Sie auch für unwirksame Dienstpläne einsetzen. Die Wirksamkeit der Zuweisungen wird in den Tabellen `AADUserHasDeneiedService` und `AADBaseTreeHasDeniedService` über die Spalte `XIsInEffect` abgebildet.

Voraussetzungen

- Der Konfigurationsparameter „`QER\Structures\Inherit\GroupExclusion`“ ist aktiviert.
- Sich ausschließende unwirksamen Dienstpläne gehören zum selben Mandanten.

Um unwirksame Dienstpläne auszuschließen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den unwirksamen Dienstplan.
3. Wählen Sie die Aufgabe **Unwirksame Dienstpläne ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die unwirksamen Dienstpläne zu, die sich mit dem gewählten Dienstplan ausschließen.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die unwirksamen Dienstpläne, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Vererbung von unwirksamen Azure® Active Directory® Dienstplänen anhand von Kategorien

Das unter [Vererbung von Azure® Active Directory® Gruppen anhand von Kategorien](#) auf Seite 100 beschriebene Verhalten können Sie auch für unwirksame Dienstpläne einsetzen.

Um die Vererbung über Kategorien zu nutzen

- Definieren Sie am Mandanten die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den unwirksamen Dienstplänen über ihre Stammdaten zu.

Verwandte Themen

- [Festlegen der Kategorien für die Vererbung von Berechtigungen auf Seite 63](#)
- [Allgemeine Stammdaten eines Azure® Active Directory® Benutzerkontos auf Seite 72](#)
- [Bearbeiten der Stammdaten von unwirksamen Azure® Active Directory® Dienstplänen auf Seite 123](#)

Zusatzeigenschaften an einen unwirksamen Azure® Active Directory® Dienstplan zuweisen

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

Um Zusatzeigenschaften für einen unwirksamen Dienstplan festzulegen

1. Wählen Sie die Kategorie **Azure® Active Directory® | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Zusatzeigenschaften.
5. Speichern Sie die Änderungen.

Verwandte Themen

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

Berichte über Azure® Active Directory® Objekte

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


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

Tabelle 43: Berichte für das Zielsystem

Bericht	Beschreibung
Übersicht aller Zuweisungen	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Mandanten mindestens ein Benutzerkonto besitzen.
Unverbundene Benutzerkonten anzeigen	Der Bericht zeigt alle Benutzerkonten des Mandanten, denen keine Person zugeordnet ist. Der Bericht enthält die Gruppenmitgliedschaften und die Risikoeinschätzung.
Personen mit mehreren Benutzerkonten anzeigen	Der Bericht zeigt alle Personen, die mehrere Benutzerkonten im Mandanten besitzen. Der Bericht enthält eine Risikoeinschätzung.
Ungenutzte Benutzerkonten anzeigen	Der Bericht enthält alle Benutzerkonten des Mandanten, die in den letzten Monaten nicht verwendet wurden. Der Bericht enthält die Gruppenmitgliedschaften und die Risikoeinschätzung.
Abweichende Systemberechtigungen anzeigen	Der Bericht enthält alle Gruppen des Mandanten, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager.
Benutzerkonten mit einer überdurchschnittlichen Anzahl an Systemberechtigungen anzeigen	Der Bericht enthält alle Benutzerkonten des Mandanten, die eine überdurchschnittliche Anzahl an Gruppenmitgliedschaften besitzen.
Azure® Active Directory® Benutzerkonten- und Gruppenverteilung	Der Bericht enthält eine Zusammenfassung zur Benutzerkonten- und Gruppenverteilung aller Mandanten. Den Bericht finden Sie in der Kategorie Mein One Identity Manager .
Datenqualität der Azure® Active Directory® Benutzerkonten	Der Bericht enthält verschiedenen Auswertungen zur Datenqualität der Benutzerkonten aller Mandanten. Den Bericht finden Sie in der Kategorie Mein One Identity Manager .

Übersicht aller Zuweisungen


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


Beispiele

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

Um detaillierte Informationen über Zuweisungen anzuzeigen

- Um den Bericht anzuzeigen, wählen Sie in der Navigation oder in der Ergebnisliste das Basisobjekt und wählen Sie den Bericht **Übersicht aller Zuweisungen**.

- Wählen Sie über die Schaltfläche  **Verwendet von** in der Symbolleiste des Berichtes, die Rollenklasse (Abteilung, Kostenstelle, Standort, Geschäftsrolle oder IT Shop Struktur), für die Sie ermitteln möchten, ob es Rollen gibt, in denen sich Personen mit dem ausgewählten Basisobjekt befinden.

Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Personen befinden, denen das ausgewählte Basisobjekt zugewiesen ist. Die Bedeutung der Steuerelemente des Berichtes ist in einer separaten Legende erläutert. Die Legende erreichen Sie über das Symbol  in der Symbolleiste des Berichtes.



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

Abbildung 3: Symbolleiste des Berichtes „Übersicht aller Zuweisungen“

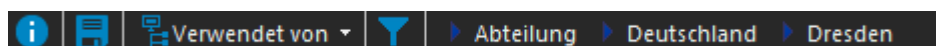





Tabelle 44: Bedeutung der Symbole in der Symbolleiste des Berichts

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

Anhang: Konfigurationsparameter für die Verwaltung einer Azure® Active Directory®-Umgebung

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

Tabelle 45: Konfigurationsparameter

Konfigurationsparameter	Beschreibung
TargetSystem\AzureAD	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung des Zielsystems Azure® Active Directory®. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.
TargetSystem\AzureAD\Accounts	Der Konfigurationsparameter erlaubt die Konfiguration der Angaben zu Benutzerkonten.
TargetSystem\AzureAD\Accounts\InitialPassword	Der Konfigurationsparameter enthält das initiale Kennwort für neu erzeugte Benutzerkonten. Wird beim Anlegen im Benutzerkonto selbst kein Kennwort angegeben, dann wird das initiale Kennwort aus dem Konfigurationsparameter benutzt. Dies kann erforderlich sein, wenn ein Benutzerkonto im Zielsystem angelegt werden muss und die Zielsystemumgebung eine minimale Kennwortlänge > 0 erfordert. Für das initiale Kennwort ist die minimale Kennwortlänge zu beachten.
TargetSystem\AzureAD\Accounts\InitialRandomPassword	Der Konfigurationsparameter legt fest, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in den Konfigurationsparametern unterhalb gesetzt sind.
TargetSystem\AzureAD\Accounts\InitialRandomPassword\Character	Der Konfigurationsparameter legt fest, ob das Zufallskennwort mindestens einen Buchstaben [a-z] enthalten muss.
TargetSystem\AzureAD\Accounts\InitialRandomPassword\Length	Der Konfigurationsparameter legt fest, wie viele Zeichen das Zufallskennwort enthalten muss.

Konfigurationsparameter	Beschreibung
TargetSystem\AzureAD\Accounts\ InitialRandomPassword\Numeric	Der Konfigurationsparameter legt fest, ob im Zufallskennwort mindestens eine Ziffer [0-9] enthalten sein muss.
TargetSystem\AzureAD\Accounts\ InitialRandomPassword\SendTo	Der Konfigurationsparameter enthält die Person, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Rolle, Verantwortlicher der Person oder XUserInserted). Ist kein Empfänger ermittelbar, dann wird an die im Konfigurationsparameter "TargetSystem\AzureAD\DefaultAddress" hinterlegte Adresse versandt.
TargetSystem\AzureAD\Accounts\ InitialRandomPassword\SendTo\ MailTemplateAccountName	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den initialen Anmeldeinformationen (Name des Benutzerkontos) zu versorgen.
TargetSystem\AzureAD\Accounts\ InitialRandomPassword\SendTo\ MailTemplatePassword	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den initialen Anmeldeinformationen (initiales Kennwort) zu versorgen.
TargetSystem\AzureAD\Accounts\ InitialRandomPassword\ SpecialCharacter	Der Konfigurationsparameter legt fest, ob im Zufallskennwort mindestens ein Sonderzeichen enthalten sein muss.
TargetSystem\AzureAD\Accounts\ MailTemplateDefaultValues	Der Konfigurationsparameter enthält die Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden.
TargetSystem\AzureAD\Accounts\ InitialRandomPassword\UpperCase	Der Konfigurationsparameter legt fest, ob im Zufallskennwort mindestens einen Großbuchstaben [A-Z] enthalten sein muss.
TargetSystem\AzureAD\Accounts\ PrivilegedAccount	Der Konfigurationsparameter erlaubt die Konfiguration der Einstellungen für privilegierte Azure® Active Directory® Benutzerkonten.
TargetSystem\AzureAD\Accounts\ PrivilegedAccount\ AccountName_Postfix	Der Konfigurationsparameter enthält den Postfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem\AzureAD\Accounts\ PrivilegedAccount\ AccountName_Prefix	Der Konfigurationsparameter enthält den Präfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem\AzureAD\DefaultAddress	Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem\AzureAD\ MaxFullsyncDuration	Der Konfigurationsparameter enthält die maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.

Konfigurationsparameter	Beschreibung
TargetSystem\AzureAD\ PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem\AzureAD\ PersonAutoDisabledAccounts	Der Konfigurationsparameter legt fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem\AzureAD\ PersonAutoFullSync	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem\AzureAD\ PersonExcludeList	<p>Der Konfigurationsparameter enthält eine Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe () getrennten Liste, die als reguläres Suchmuster verarbeitet wird.</p> <p>Beispiel:</p> <p>ADMINISTRATOR</p>

Anhang: Standardprojektvorlage für Azure® Active Directory®

Eine Standardprojektvorlage sorgt dafür, dass alle benötigten Informationen im One Identity Manager angelegt werden. Dazu gehören beispielsweise die Mappings, Workflows und das Basisobjekt der Synchronisation. Wenn Sie keine Standardprojektvorlage verwenden, müssen Sie das Basisobjekt der Synchronisation selbst im One Identity Manager bekannt geben.

Verwenden Sie eine Standardprojektvorlage für die initiale Einrichtung des Synchronisationsprojektes. Für kundenspezifische Implementierungen können Sie das Synchronisationsprojekt mit dem Synchronization Editor erweitern.

Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 46: Abbildung der Azure® Active Directory® Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im Azure® Active Directory®	Tabelle im One Identity Manager Schema
DirectoryRole	AADDirectoryRole
Group	AADGroup
LicenseAssignments	AADUserHasSubSku
Organization	AADOrganization
ServicePlans	AADServicePlan
SubscribedSku	AADSubSku
User	AADUser
Verified Domain	AADVerifiedDomain

Dell berücksichtigt die Wünsche seiner Kunden und liefert auf der ganzen Welt innovative Technologien, Geschäftslösungen und Dienstleistungen, die anerkannt und geschätzt werden. Weitere Informationen finden Sie unter www.quest.com.

Kontaktaufnahme zu Dell

Bei Fragen zum Kauf von Dell Produkten oder anderen Fragen besuchen Sie <http://quest.com/company/contact-us.aspx> oder rufen Sie +1 949 754 8000 an.

Technische Supportressourcen

Der technische Support steht Kunden, die Dell-Software mit einem gültigen Wartungsvertrag gekauft haben, und Kunden zur Verfügung, die über eine Testversion verfügen. Das Support Portal ist unter <https://support.quest.com/> erreichbar.

Das Support Portal stellt Selbsthilfetools bereit, mit denen Sie Probleme schnell und eigenständig lösen können - 24 Stunden am Tag, 365 Tage im Jahr. Darüber hinaus ermöglicht das Portal über ein Online-Serviceanforderungssystem auch direkten Zugang zu unseren Produktsupporttechnikern.

Das Portal bietet folgende Möglichkeiten:

- Erstellen, Aktualisieren und Verwalten von Serviceanforderungen (Supportfälle)
- Anzeigen von Knowledge Base-Artikeln
- Erhalten von Produktbenachrichtigungen
- Herunterladen von Software. Testsoftware finden Sie unter <http://quest.com/trials>.
- Anzeigen von Videos zur Vorgehensweise
- Teilnahme an Communitydiskussionen
- Chatten mit einem Supporttechniker

A

- Anmeldeinformationen 52
- Architekturüberblick 7
- Ausschlussdefinition 98, 121, 130
- Ausstehendes Objekt 27
- Azure® Active Directory®
 - Anwendung 13
- Azure® Active Directory® Abonnement 113
 - an Abteilung zuweisen 115
 - an Geschäftsrolle zuweisen 117
 - an Kostenstelle zuweisen 115
 - an Standort zuweisen 115
 - ausschließen 121
 - bearbeiten 113
 - Benutzerkonto zuweisen 79, 115, 117, 124
 - in IT Shop aufnehmen 119
 - in Systemrolle aufnehmen 118
 - Kategorie 122
 - wirksam 121
 - Zusatzeigenschaft zuweisen 122, 131
- Azure® Active Directory® Administratorrolle 104
 - an Abteilung zuweisen 106
 - an Geschäftsrolle zuweisen 107
 - an Kostenstelle zuweisen 106
 - an Standort zuweisen 106
 - Anzeigenname 104
 - bearbeiten 104
 - Benutzerkonto zuweisen 78, 105, 108
 - in IT Shop aufnehmen 110
 - in Systemrolle aufnehmen 109
 - Kategorie 104, 112
 - Leistungsposition 104
 - Mandant 104
 - Risikoindex 104
 - Vorlage 104
 - Zusatzeigenschaft zuweisen 112
- Azure® Active Directory® Benutzerkonto
 - Abonnement zuweisen 79, 117
 - Abteilung 75
 - administratives Benutzerkonto 67
 - Administratorrolle zuweisen 78, 108
 - Alias 72
 - Anmeldename 72
 - Automatisierungsgrad 72, 77
 - Berufsbezeichnung 75
 - deaktivieren 72, 85
 - Domäne 72
 - E-Mail-Adresse 72, 75
 - einrichten 71
 - Firma 75
 - Gruppe zuweisen 78, 94
 - Gruppen erben 72
 - Identität 67, 72
 - Kategorie 72, 100, 112, 122, 130
 - Kennwort 72
 - initial 50
 - Kennwortrichtlinien 72
 - Kontendefinition 48, 72
 - Kontomanager 75
 - Lokales Benutzerkonto 76
 - löschen 86
 - Mandant 72
 - Ort 75
 - Person 72
 - Person zuweisen 66, 71-72, 81
 - privilegiertes Benutzerkonto 67, 72
 - Proxy Adressen 75
 - Risikoindex 72
 - SID 76
 - sperrern 86
 - Standardbenutzerkonto 67
 - Standort 72
 - Typ 67

- Unveränderlicher Bezeichner 76
 - unwirksamen Dienstplan zuweisen 79, 126
 - verwalten 66
 - wiederherstellen 86
 - Zusatzeigenschaft zuweisen 80
 - Azure® Active Directory® Dienstplan 113, 115
 - Unwirksamer Dienstplan
 - an Abteilung zuweisen 124
 - an Geschäftsrolle zuweisen 125
 - an Kostenstelle zuweisen 124
 - an Standort zuweisen 124
 - ausschließen 130
 - bearbeiten 123
 - Benutzerkonto zuweisen 79, 124, 126
 - in IT Shop aufnehmen 119, 128
 - in Systemrolle aufnehmen 127
 - Kategorie 130
 - wirksam 130
 - Azure® Active Directory® Domäne 64
 - Azure® Active Directory® Gruppe
 - Alias 89
 - an Abteilung zuweisen 92
 - an Geschäftsrolle zuweisen 93
 - an Kostenstelle zuweisen 92
 - an Standort zuweisen 92
 - ausschließen 98
 - bearbeiten 89
 - Benutzerkonto zuweisen 78, 91, 94
 - E-Mail-Adresse 89
 - E-Mail aktivierte Sicherheitsgruppe 88
 - Eigentümer 102
 - Gruppe zuweisen 97
 - Gruppentyp 88-89
 - in IT Shop aufnehmen 95
 - in Systemrolle aufnehmen 94
 - Kategorie 89, 100
 - Leistungsposition 89
 - löschen 103
 - Mandant 89
 - Office 365 Gruppe 88
 - Risikoindex 89
 - Sicherheitsgruppe 88-89
 - Verteilerguppe 88
 - wirksam 98
 - Zusatzeigenschaft zuweisen 102
 - Azure® Active Directory® Lizenz 113
 - Azure® Active Directory® Mandant
 - Anwendungsrollen 8
 - bearbeiten 60
 - Berichte 132
 - Kategorie 63, 100, 112, 122, 130
 - Kontendefinition 61
 - Kontendefinition (initial) 48
 - Lokales Active Directory® 62
 - Personenzuordnung 83
 - Synchronisation 61
 - Übersicht aller Zuweisungen 133
 - Zielsystemverantwortlicher 8, 53, 61
- ## B
- Benachrichtigung 52
 - Benutzerkonto
 - administratives Benutzerkonto 67
 - Bildungsregeln ausführen 42
 - Identität 67
 - Kennwort
 - Benachrichtigung 52
 - privilegiertes Benutzerkonto 67
 - Standardbenutzerkonto 67
 - Typ 67
 - Bildungsregel
 - IT Betriebsdaten ändern 42
- ## E
- E-Mail-Benachrichtigung 52

I

IT Betriebsdaten

ändern 42

IT Shop Regal

Kontendefinitionen zuweisen 46

J

Jobserver

bearbeiten 13

K

Kennwort

initial 52

Konfigurationsparameter 135

Kontendefinition 33

an Abteilung zuweisen 43

an alle Personen zuweisen 44

an Azure® Active Directory® Mandant
zuweisen 48

an Geschäftsrolle zuweisen 44

an Kostenstelle zuweisen 43

an Person zuweisen 42, 45

an Standort zuweisen 43

an Systemrollen zuweisen 46

automatisch zuweisen 44

Automatisierungsgrad 36

erstellen 34

in IT Shop aufnehmen 46

IT Betriebsdaten 39-40

löschen 48

M

Mitgliedschaft

Änderung provisionieren 29

O

Objekt

ausstehend 27

publizieren 27

sofort löschen 27

One Identity Manager

Administrator 8

als Anwendung registrieren 13

Benutzer 8

Zielsystemadministrator 8

Zielsystemverantwortlicher 8, 53

P

Personenzuordnung

automatisch 81

entfernen 83

manuell 83

Suchkriterium 83

Tabellenspalte 83

Projektvorlage 138

Provisionierung

Mitgliederliste 29

S

Schema

aktualisieren 26

Änderungen 26

komprimieren 26

Synchronisation

Basisobjekt

erstellen 26

Benutzer 12

Berechtigungen 12

einrichten 11

Erweitertes Schema 26

konfigurieren 17, 24

Scope 24

starten 17

Synchronisationsprojekt

erstellen 17

Variable 24

Variablenset 26

- Verbindungsparameter 17, 24, 26
- verhindern 31
- verschiedene Domänen 26
- Workflow 17, 25
- Zielsystemschemata 26
- Synchronisationsanalysebericht 30
- Synchronisationskonfiguration
 - anpassen 24-26
- Synchronisationsprojekt
 - bearbeiten 64
 - deaktivieren 31
 - erstellen 17
 - Projektvorlage 138
- Synchronisationsprotokoll 23
- Synchronisationsrichtung
 - In das Zielsystem 17, 25
 - In den Manager 17
- Synchronisationsserver
 - installieren 13
 - Jobserver 13
 - konfigurieren 13
- Synchronisationsworkflow
 - erstellen 17, 25

Z

- Zeitplan
 - deaktivieren 31
- Zielsystemabgleich 27