



One Identity Manager 8.2.1

Administrationshandbuch für die
Anbindung einer Microsoft Teams-
Umgebung

Copyright 2022 One Identity LLC.

ALLE RECHTE VORBEHALTEN.

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

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

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

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

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

Patente

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

Marken

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

Legende

-  **WARNUNG:** Das Symbol **WARNUNG** weist auf ein potenzielles Risiko von Körperverletzungen oder Sachschäden hin, für das Sicherheitsvorkehrungen nach Industriestandard empfohlen werden. Dieses Symbol ist oft verbunden mit elektrischen Gefahren bezüglich Hardware.
-  **VORSICHT:** Das Symbol **VORSICHT** weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.

One Identity Manager Administrationshandbuch für die Anbindung einer Microsoft Teams-Umgebung
Aktualisiert - 27. April 2022, 02:58 Uhr
Version - 8.2.1

Inhalt

Über dieses Handbuch	5
Verwalten einer Microsoft Teams-Umgebung	6
Architekturüberblick	6
One Identity Manager Benutzer für die Verwaltung einer Microsoft Teams-Umgebung .	7
Synchronisieren einer Microsoft Teams-Umgebung	10
Einrichten der Initialsynchronisation mit Microsoft Teams	11
Erweitern der Berechtigungen für die One Identity Manager Anwendung im Azure Active Directory Mandanten	12
Benutzer und Berechtigungen für die Synchronisation mit Microsoft Teams	13
Einrichten des Synchronisationservers für Microsoft Teams	14
Systemanforderungen für den Synchronisationsserver für Microsoft Teams	15
One Identity Manager Service für die Synchronisation mit Microsoft Teams instal- lieren	15
Erstellen eines Synchronisationsprojektes für die initiale Synchronisation mit Microsoft Teams	18
Benötigte Informationen für Synchronisationsprojekte mit Microsoft Teams	19
Initiales Synchronisationsprojekt für die Synchronisation mit Microsoft Teams erstellen	21
Synchronisationsprotokoll konfigurieren	25
Anpassen der Synchronisationskonfiguration für Microsoft Teams	26
Synchronisation in die Microsoft Teams-Umgebung konfigurieren	27
Einstellungen der Systemverbindung zur Microsoft Teams-Umgebung ändern	28
Verbindungsparameter im Variablenset bearbeiten	28
Eigenschaften der Zielsystemverbindung bearbeiten	29
Schema aktualisieren	30
Einzelobjektsynchronisation konfigurieren	31
Beschleunigung der Provisionierung und Einzelobjektsynchronisation	32
Ausführen einer Synchronisation	34
Synchronisationen starten	34
Synchronisation deaktivieren	35
Synchronisationsergebnisse anzeigen	36
Einzelobjekte synchronisieren	37

Aufgaben nach einer Synchronisation	37
Ausstehende Objekte nachbehandeln	37
Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen	39
Fehleranalyse	40
Datenfehler bei der Synchronisation ignorieren	41
Abbildung von Microsoft Teams Objekten im One Identity Manager	42
Microsoft Teams Teams	42
Microsoft Teams Teams erstellen	43
Stammdaten für Microsoft Teams Teams bearbeiten	44
Microsoft Teams Teams archivieren	44
Microsoft Teams Teams löschen	44
Zuweisen von Microsoft Teams Teams an Azure Active Directory Benutzerkonten ...	45
Microsoft Teams Teams automatisch in den IT Shop aufnehmen	46
Mitglieder von Microsoft Teams Teams anzeigen	47
Eigentümer von Microsoft Teams Teams anzeigen	48
Überblick über Microsoft Teams Teams anzeigen	48
Stammdaten für Microsoft Teams Teams	49
Microsoft Teams Kanäle	50
Microsoft Teams Standardkanäle erstellen	51
Private Microsoft Teams Kanäle anzeigen	51
Microsoft Teams Kanäle löschen	52
Überblick über Microsoft Teams Kanäle anzeigen	53
Stammdaten für Microsoft Teams Kanäle	53
Basisdaten für die Verwaltung einer Microsoft Teams-Umgebung	54
Anhang: Konfigurationsparameter für die Verwaltung einer Microsoft Teams-Umgebung	56
Anhang: Standardprojektvorlage für Microsoft Teams	58
Anhang: Verarbeitung von Microsoft Teams Systemobjekten	59
Anhang: Bekannte Probleme bei der Anbindung von Microsoft Teams	60
Über uns	61
Kontaktieren Sie uns	61
Technische Supportressourcen	61
Index	62

Über dieses Handbuch

Das *One Identity Manager Administrationshandbuch für die Anbindung einer Microsoft Teams-Umgebung* beschreibt, wie Sie die Synchronisation einer Microsoft Teams-Umgebung mit dem One Identity Manager einrichten. Sie erfahren, wie im One Identity Manager die Teams und Kanäle einer Microsoft Teams-Umgebung abgebildet werden.

Ausführliche Informationen zu Microsoft Teams finden Sie in der *Microsoft Teams Dokumentation* von Microsoft. Ausführliche Informationen zum Synchronisieren eines Azure Active Directory Mandanten finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung*. Ausführliche Informationen zum Synchronisieren einer Exchange Online Organisation finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung*.

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

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

Verfügbare Dokumentation

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

Verwalten einer Microsoft Teams-Umgebung

Im One Identity Manager werden die Teams und Kanäle einer Microsoft Teams-Umgebung abgebildet. In einem Team werden Microsoft Teams Benutzer wie in einer Gruppe zusammengefasst. Ein Team ist mit einer Exchange Online Office 365 Gruppe verbunden. Alle Mitglieder der Office 365 Gruppe sind Mitglieder des Teams. Die Mitglieder eines Teams können die Kanäle des Teams nutzen. Standardkanäle sind für alle Mitglieder des Teams zugänglich. Private Kanäle sind nur für bestimmte Mitglieder des Teams zugänglich. Mitglieder eines Teams, die nicht in den privaten Kanal eingeladen wurden, sehen diesen Kanal nicht.

Damit die Benutzer Microsoft Teams nutzen können, benötigen Sie einen Microsoft Teams Dienstplan. Ausführliche Informationen zu Microsoft Teams finden Sie in der *Microsoft Teams Dokumentation* von Microsoft.

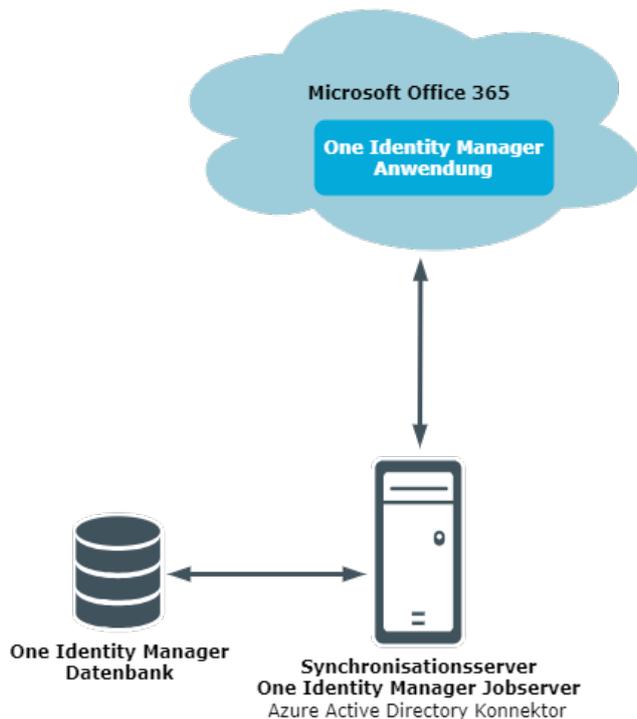
HINWEIS: Voraussetzung für die Verwaltung einer Microsoft Teams-Umgebung im One Identity Manager ist die Installation des Microsoft Teams Moduls. Ausführliche Informationen zur Installation finden Sie im *One Identity Manager Installationshandbuch*.

Architekturüberblick

Die Synchronisation mit der Microsoft Teams-Umgebung übernimmt der Azure Active Directory Konnektor. Der Azure Active Directory Konnektor wird auf einem Synchronisationsserver installiert. Der Synchronisationsserver sorgt für den Abgleich der Daten zwischen der One Identity Manager-Datenbank und Microsoft Teams.

Der Azure Active Directory Konnektor ist Bestandteil des Azure Active Directory Moduls. Mit der Installation des Microsoft Teams Moduls wird die Synchronisationsvorlage für Microsoft Teams bereitgestellt. Der Azure Active Directory Konnektor verwendet die Microsoft Graph-API für den Zugriff auf Microsoft Teams.

Abbildung 1: Architektur für die Synchronisation



HINWEIS: Für den Zugriff auf Microsoft Teams Daten müssen der Azure Active Directory Mandant und die Exchange Online Organisation synchronisiert werden.

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

One Identity Manager Benutzer für die Verwaltung einer Microsoft Teams-Umgebung

In die Einrichtung und Verwaltung einer Microsoft Teams-Umgebung sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Zielsystemadministratoren	Die Zielsystemadministratoren müssen der

Benutzer

Aufgaben

Anwendungsrolle **Zielsysteme | Administratoren** zugewiesen sein.

Benutzer mit dieser Anwendungsrolle:

- Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen.
- Legen die Zielsystemverantwortlichen fest.
- Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein.
- Legen fest, welche Anwendungsrollen für Zielsystemverantwortliche sich ausschließen.
- Berechtigen weitere Personen als Zielsystemadministratoren.
- Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.

Zielsystemverantwortliche Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Exchange Online** oder einer untergeordneten Anwendungsrolle zugewiesen sein.

Benutzer mit dieser Anwendungsrolle:

- Übernehmen die administrativen Aufgaben für das Zielsystem.
- Erzeugen, ändern oder löschen die Zielsystemobjekte.
- Bearbeiten Kennwortrichtlinien für das Zielsystem.
- Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**.
- Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.
- Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation.
- Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

One Identity Manager Administratoren

One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen.

One Identity Manager Administratoren:

Benutzer

Aufgaben

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

Synchronisieren einer Microsoft Teams-Umgebung

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

Informieren Sie sich hier:

- wie Sie die Synchronisation einrichten, um initial Daten aus eine Microsoft Teams-Umgebung in die One Identity Manager-Datenbank einzulesen,
- wie Sie eine Synchronisationskonfiguration anpassen,
- wie Sie die Synchronisation starten und deaktivieren,
- wie Sie die Synchronisationsergebnisse auswerten.

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

Detaillierte Informationen zum Thema

- [Einrichten der Initialsynchronisation mit Microsoft Teams](#) auf Seite 11
- [Anpassen der Synchronisationskonfiguration für Microsoft Teams](#) auf Seite 26
- [Ausführen einer Synchronisation](#) auf Seite 34
- [Aufgaben nach einer Synchronisation](#) auf Seite 37
- [Fehleranalyse](#) auf Seite 40
- [Datenfehler bei der Synchronisation ignorieren](#) auf Seite 41
- [Verarbeitung von Microsoft Teams Systemobjekten](#) auf Seite 59

Einrichten der Initialsynchronisation mit Microsoft Teams

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

Voraussetzungen für die Synchronisation einer Microsoft Teams-Umgebung sind:

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

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

Um die Objekte einer Microsoft Teams initial in die One Identity Manager-Datenbank einzulesen

1. Erweitern Sie die registrierte One Identity Manager Anwendung im Azure Active Directory Mandanten um zusätzliche Berechtigungen.
2. Die One Identity Manager Bestandteile für die Verwaltung von Microsoft Teams-Umgebungen sind verfügbar, wenn der Konfigurationsparameter **TargetSystem | AzureAD | ExchangeOnline | Teams** aktiviert ist.
 - Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.
HINWEIS: Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
3. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
4. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Detaillierte Informationen zum Thema

- [Erweitern der Berechtigungen für die One Identity Manager Anwendung im Azure Active Directory Mandanten](#) auf Seite 12
- [Benutzer und Berechtigungen für die Synchronisation mit Microsoft Teams](#) auf Seite 13
- [Einrichten des Synchronisationservers für Microsoft Teams](#) auf Seite 14
- [Erstellen eines Synchronisationsprojektes für die initiale Synchronisation mit Microsoft Teams](#) auf Seite 18
- [Synchronisationsprotokoll konfigurieren](#) auf Seite 25
- [Standardprojektvorlage für Microsoft Teams](#) auf Seite 58

Erweitern der Berechtigungen für die One Identity Manager Anwendung im Azure Active Directory Mandanten

Die Berechtigungen für die Anwendung für den One Identity Manager können Sie im Microsoft Azure Portal (<https://portal.azure.com/>) oder im Azure Active Directory Admin Center (<https://admin.microsoft.com/>) erweitern.

Für die Synchronisation zwischen One Identity Manager und Azure Active Directory haben Sie bereits eine One Identity Manager-Anwendung im Azure Active Directory Mandanten registriert. Für die Synchronisation mit Microsoft Teams müssen Sie die Berechtigungen für diese Anwendung erweitern.

- Wenn Sie die Authentifizierung im Kontext eines Verzeichnisbenutzers nutzen (delegierte Berechtigungen), weisen Sie zusätzlich die delegierte Berechtigung **ChannelMember.Read.All** (Read the members of channels) zu.
- Wenn Sie die Authentifizierung im Kontext einer Anwendung nutzen (Anwendungsberechtigungen), weisen Sie zusätzlich die Anwendungsberechtigung **ChannelMember.Read.All** (Read the members of all channels) zu.

Ausführliche Informationen zum Registrieren einer Unternehmensanwendung für den One Identity Manager im Azure Active Directory Mandant und zum Zuweisen der Berechtigungen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung*.

Verwandte Themen

- [Benutzer und Berechtigungen für die Synchronisation mit Microsoft Teams](#) auf Seite 13

Benutzer und Berechtigungen für die Synchronisation mit Microsoft Teams

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 Azure Active Directory oder Wert des geheimen Schlüssels	<p>Abhängig davon, wie die Anwendung für den One Identity Manager im Azure Active Directory Mandanten registriert ist, wird entweder ein Benutzerkonto mit ausreichenden Berechtigungen oder der geheime Schlüssel benötigt.</p> <ul style="list-style-type: none">• Wenn Sie die Authentifizierung im Kontext eines Verzeichnisbenutzers nutzen (delegierte Berechtigungen), benötigen Sie bei der Einrichtung des Synchronisationsprojektes ein Benutzerkonto, welches Mitglied in der Azure Active Directory Administratorrolle Globaler Administrator ist. Die Zuweisung der Azure Active Directory Administratorrolle an das Benutzerkonto nehmen Sie im Azure Active Directory Admin Center vor. Ausführliche Informationen zum Verwalten von Berechtigungen in Azure Active Directory finden Sie in der <i>Microsoft Dokumentation</i>. <p>HINWEIS: Das Benutzerkonto für den Zugriff auf Azure Active Directory darf keine Multifaktor-Authentifizierung nutzen, damit automatisierte Anmeldungen in einem Benutzerkontext möglich sind.</p> <p>Zusätzlich muss das Benutzerkonto eine Lizenz mit dem Dienst Teams besitzen.</p> <ul style="list-style-type: none">• Wenn Sie die Authentifizierung im Kontext einer Anwendung nutzen (Anwendungsberechtigungen), benötigen Sie bei der Einrichtung des Synchronisationsprojektes den Wert des geheimen Schlüssels. Der geheime Schlüssel, wird bei der Registrierung des One Identity Manager als Anwendung des Azure Active Directory Mandanten erzeugt. <p>HINWEIS: Der Schlüssel ist nur begrenzte Zeit gültig und muss nach Ablauf ausgetauscht werden.</p>
Benutzerkonto des One Identity Manager Service	<p>Das Benutzerkonto für den One Identity Manager Service benötigt die Benutzerrechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Verzeichnisse und Dateien anlegen und bearbeiten.</p> <p>Das Benutzerkonto muss der Gruppe Domänen-Benutzer angehören.</p> <p>Das Benutzerkonto benötigt das erweiterte Benutzerrecht Anmelden als Dienst.</p>

Benutzer	Berechtigungen
Benutzer für den Zugriff auf die One Identity Manager-Datenbank	<p>Das Benutzerkonto benötigt Berechtigungen 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 Berechtigungen für den internen Webservice über folgenden Kommandozeilenaufruf vergeben:</p> <pre>netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis.</p> <p>In der Standardinstallation wird der One Identity Manager installiert unter:</p> <ul style="list-style-type: none"> • %ProgramFiles(x86)%\One Identity (auf 32-Bit Betriebssystemen) • %ProgramFiles%\One Identity (auf 64-Bit Betriebssystemen) <p>Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer Synchronization bereitgestellt.</p>

Verwandte Themen

- [Erweitern der Berechtigungen für die One Identity Manager Anwendung im Azure Active Directory Mandanten](#) auf Seite 12

Einrichten des Synchronisationsservers für Microsoft Teams

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 werden.

Detaillierte Informationen zum Thema

- [Systemanforderungen für den Synchronisationsserver für Microsoft Teams](#) auf Seite 15
- [One Identity Manager Service für die Synchronisation mit Microsoft Teams installieren](#) auf Seite 15

Systemanforderungen für den Synchronisationsserver für Microsoft Teams

Für die Einrichtung der Synchronisation mit einem Microsoft Teams muss ein Server zur Verfügung gestellt werden, auf dem die nachfolgend genannte Software installiert ist:

- Windows Betriebssystem
Unterstützt werden die Versionen:
 - Windows Server 2022
 - Windows Server 2019
 - Windows Server 2016
 - Windows Server 2012 R2
 - Windows Server 2012
- Microsoft .NET Framework Version 4.7.2 oder höher
| **HINWEIS:** Beachten Sie die Empfehlungen des Zielsystemherstellers.

One Identity Manager Service für die Synchronisation mit Microsoft Teams installieren

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.

Tabelle 3: Eigenschaften des Jobservers

Eigenschaft	Wert
Serverfunktion	Azure Active Directory Konnektor
Maschinenrolle	Server Jobserver Azure Active Directory

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

gleichartige Aufträge von einem Jobserver zu verarbeiten sind (Nachnutzung bestehender Verbindungen).

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

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

HINWEIS: Das Programm führt eine Remote-Installation des One Identity Manager Service aus. Eine lokale Installation des Dienstes ist mit diesem Programm nicht möglich.

Für die Remote-Installation des One Identity Manager Service benötigen Sie eine administrative Arbeitsstation, auf der die One Identity Manager-Komponenten installiert sind.

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

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

1. Starten Sie das Programm Server Installer auf Ihrer administrativen Arbeitsstation.
2. Auf der Seite **Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.
3. Auf der Seite **Servereigenschaften** legen Sie fest, auf welchem Server der One Identity Manager Service installiert werden soll.
 - a. Wählen Sie in der Auswahlliste **Server** einen Jobserver aus.
- ODER -
Um einen neuen Jobserver zu erstellen, klicken Sie **Hinzufügen**.
 - b. Bearbeiten Sie folgende Informationen für den Jobserver.
 - **Server:** Bezeichnung des Jobservers.
 - **Queue:** Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder Jobserver innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert.

Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.

- **Vollständiger Servername:** Vollständiger Servername gemäß DNS Syntax.

Syntax:

<Name des Servers>.<Vollqualifizierter Domänenname>

HINWEIS: Über die Option **Erweitert** können Sie weitere Eigenschaften für den Jobserver bearbeiten.

4. Auf der Seite **Maschinenrollen** wählen Sie **Azure Active Directory**.
5. Auf der Seite **Serverfunktionen** wählen Sie **Azure Active Directory Konnektor (via Microsoft Graph)**.
6. Auf der Seite **Dienstkonfiguration** erfassen Sie die Verbindungsinformationen und prüfen Sie die Konfiguration des One Identity Manager Service.

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

- Für eine direkte Verbindung zu Datenbank:
 1. Wählen Sie **Prozessabholung > sqlprovider**
 2. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
 3. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
 - Für eine Verbindung zum Anwendungsserver:
 1. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
 2. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
 3. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.
 4. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
 5. Wählen Sie das Authentifizierungsmodul. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
7. Zur Konfiguration der Remote-Installation, klicken Sie **Weiter**.
 8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
 9. Auf der Seite **Installationsquelle festlegen** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.

10. Wenn die Datenbank verschlüsselt ist, wählen Sie auf der Seite **Datenbankschlüsseldatei auswählen** die Datei mit dem privaten Schlüssel.
11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
 - **Computer:** Erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
 - **Dienstkonto:** Erfassen Sie die Angaben zum Benutzerkonto unter dem der One Identity Manager Service läuft. Erfassen Sie das Benutzerkonto, das Kennwort zum Benutzerkonto und die Kennwortwiederholung.

Die Installation des Dienstes erfolgt mit dem Benutzerkonto, mit dem Sie an der administrativen Arbeitsstation angemeldet sind. Möchten Sie ein anderes Benutzerkonto für die Installation des Dienstes nutzen, können Sie dieses in den erweiterten Optionen eintragen. Angaben zum One Identity Manager Service können Sie ebenfalls über die erweiterten Optionen ändern, beispielsweise das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den One Identity Manager Service.

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

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

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

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation mit Microsoft Teams

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

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

Voraussetzungen für die Erstellung eines Synchronisationsprojektes

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

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

Verwandte Themen

- [Benötigte Informationen für Synchronisationsprojekte mit Microsoft Teams](#) auf Seite 19
- [Initiales Synchronisationsprojekt für die Synchronisation mit Microsoft Teams erstellen](#) auf Seite 21

Benötigte Informationen für Synchronisationsprojekte mit Microsoft Teams

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

Tabelle 4: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Anwendungs-ID	Die Anwendungs-ID wird beim Registrieren der One Identity Manager-Anwendung im Azure Active Directory Mandanten erzeugt.
Anmeldedomäne	Azure Active Directory Name der Domäne zur Anmeldung am Azure Active Directory. Sie können die Basisdomäne oder eine verifizierte Domäne Ihres Azure Active Directory Mandanten verwenden.
Benutzerkonto und Kennwort zur Anmeldung oder Wert des geheimen Schlüssels	Abhängig davon, wie die One Identity Manager-Anwendung im Azure Active Directory Mandanten registriert ist, wird entweder ein Benutzerkonto mit ausreichenden Berechtigungen oder der geheime Schlüssel benötigt. Weitere Informationen finden Sie unter Benutzer und Berechtigungen für die Synchronisation mit Microsoft Teams auf Seite 13.

Angaben	Erläuterungen
Synchronisationsserver für Microsoft Teams	<p>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.</p> <p>Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem Azure Active Directory Konnektor installiert sein.</p> <p>Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften.</p> <ul style="list-style-type: none"> • Serverfunktion: Azure Active Directory Konnektor (via Microsoft Graph) • Maschinenrolle: Server Jobserver Azure Active Directory
Verbindungsdaten zur One Identity Manager-Datenbank	<ul style="list-style-type: none"> • Datenbankserver • Name der Datenbank • SQL Server Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung verwendet wird <p>Die Verwendung der integrierten Windows-Authentifizierung wird nicht empfohlen. Sollten Sie das Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.</p>
Remoteverbindungsserver	<p>Um die Synchronisation mit einem Zielsystem zu konfigurieren, muss der One Identity Manager Daten aus dem Zielsystem auslesen. Dabei kommuniziert der One Identity Manager direkt mit dem Zielsystem. Mitunter ist der direkte Zugriff von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, nicht möglich, beispielsweise aufgrund der Firewall-Konfiguration oder weil die Arbeitsstation nicht die notwendigen Hard- oder Softwarevoraussetzungen erfüllt. Wenn der direkte Zugriff von der Arbeitsstation nicht möglich ist, kann eine Remoteverbindung eingerichtet werden.</p> <p>Der Remoteverbindungsserver und die Arbeitsstation müssen in der selben Active Directory Domäne stehen.</p> <p>Konfiguration des Remoteverbindungservers:</p> <ul style="list-style-type: none"> • One Identity Manager Service ist gestartet

Angaben

Erläuterungen

- **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 sowie der Berechtigungen des Benutzerkontos) wie der Synchronisationsserver. Nutzen Sie den Synchronisationsserver gleichzeitig als Remoteverbindungsserver, indem Sie lediglich das **RemoteConnectPlugin** zusätzlich installieren.

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

Verwandte Themen

- [Einrichten des Synchronisationservers für Microsoft Teams](#) auf Seite 14

Initiales Synchronisationsprojekt für die Synchronisation mit Microsoft Teams erstellen

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

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

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

HINWEIS: Pro Zielsystem und genutzter Standardprojektvorlage kann genau ein Synchronisationsprojekt erstellt werden.

Um ein initiales Synchronisationsprojekt für Microsoft Teams 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** und klicken Sie **Starten**.

Der Projektassistent des Synchronization Editors wird gestartet.

3. Auf der Seite **Systemzugriff** legen Sie fest, wie der One Identity Manager auf das Zielsystem zugreifen kann.
 - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, möglich, nehmen Sie keine Einstellungen vor.
 - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, nicht möglich, können Sie eine Remoteverbindung herstellen.
Aktivieren Sie die Option **Verbindung über einen Remoteverbindungsserver herstellen** und wählen Sie unter **Jobserver** den Server, über den die Verbindung hergestellt werden soll.
4. Auf der Seite **Azure Active Directory Mandant** erfassen Sie folgende Informationen:
 - **Bereitstellung:** Wählen Sie Ihre Cloudbereitstellung. Zur Auswahl stehen **Microsoft Graph global service** und **Microsoft Cloud for US Government (L4)**.
 - **Anwendungs-ID:** Erfassen Sie die Anwendungs-ID. Die Anwendungs-ID wurde beim Registrieren der One Identity Manager-Anwendung im Azure Active Directory Mandanten erzeugt.
 - **Anmeldedomäne:** Erfassen Sie die Basisdomäne oder eine verifizierte Domäne Ihres Azure Active Directory Mandanten.
5. Auf der Seite **Authentifizierung** wählen Sie die Art der Anmeldung und erfassen die benötigten Anmeldeinformationen. Die benötigten Informationen sind abhängig davon, wie die One Identity Manager-Anwendung im Azure Active Directory Mandanten registriert ist.
 - Wenn Sie One Identity Manager als Mobilgerät- und Desktopanwendung in Ihrem Azure Active Directory Mandanten registriert haben, wählen Sie die Option **Authentifizierung als Mobilgerät- und Desktopanwendung** und erfassen Sie das Benutzerkonto und das Kennwort des Benutzerkontos zur Anmeldung.
 - Wenn Sie One Identity Manager als Webanwendung in Ihrem Azure Active Directory Mandanten integriert haben, wählen Sie die Option **Authentifizierung als Webanwendung** und erfassen Sie den Wert des geheimen Schlüssels.
Der geheime Schlüssel wurde bei der Registrierung der One Identity Manager-Anwendung des Azure Active Directory Mandanten erzeugt.
6. Auf der letzten Seite des Systemverbindungsassistenten können Sie die Verbindungsdaten speichern.
 - Aktivieren Sie die Option **Verbindung lokal speichern**, um die Verbindungsdaten zu speichern. Diese können Sie bei der Einrichtung weiterer Synchronisationsprojekte nutzen.

- Um den Systemverbindungsassistenten zu beenden und zum Projektassistenten zurückzukehren, klicken Sie **Fertig**.
7. Auf der Seite **One Identity Manager Verbindung** überprüfen Sie die Verbindungsdaten zur One Identity Manager-Datenbank. Die Daten werden aus der verbundenen Datenbank geladen. Geben Sie das Kennwort erneut ein.

HINWEIS:

 - Wenn Sie mit einer unverschlüsselten One Identity Manager-Datenbank arbeiten und noch kein Synchronisationsprojekt in der Datenbank gespeichert ist, erfassen Sie alle Verbindungsdaten neu.
 - Wenn bereits ein Synchronisationsprojekt gespeichert ist, wird diese Seite nicht angezeigt.
 8. Der Assistent lädt das Zielsystemschemata. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.
 9. Auf der Seite **Projektvorlage auswählen** wählen Sie die Projektvorlage **Microsoft Teams (via Azure Active Directory)**.
 10. Auf der Seite **Zielsystemzugriff einschränken** legen Sie fest, wie der Systemzugriff erfolgen soll. Zur Auswahl stehen:

Tabelle 5: Zielsystemzugriff festlegen

Option	Bedeutung
Das Zielsystem soll nur eingelesen werden.	<p>Gibt an, 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>Gibt an, 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

Option**Bedeutung**

Verarbeitungsmethoden nur für die Synchronisationsrichtung **In das Zielsystem** definiert.

- Synchronisationsschritte werden nur für solche Schemaklassen erstellt, deren Schematypen schreibbar sind.

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

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

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

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

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

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

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

Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

HINWEIS:

- Beim Aktivieren wird eine Konsistenzprüfung durchgeführt. Wenn dabei Fehler auftreten, erscheint eine Meldung. Sie können entscheiden, ob das Synchronisationsprojekt dennoch aktiviert werden soll.

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

- Wenn das Synchronisationsprojekt nicht sofort aktiviert werden soll, deaktivieren Sie die Option **Synchronisationsprojekt speichern und sofort aktivieren**. In diesem Fall speichern Sie das Synchronisationsprojekt manuell vor dem Beenden des Synchronization Editor.
- Die Verbindungsdaten zum Zielsystem werden in einem Variablenset gespeichert und können bei Bedarf im Synchronization Editor in der Kategorie **Konfiguration > Variablen** angepasst werden.

Verwandte Themen

- [Benutzer und Berechtigungen für die Synchronisation mit Microsoft Teams](#) auf Seite 13
- [Benötigte Informationen für Synchronisationsprojekte mit Microsoft Teams](#) auf Seite 19
- [Einrichten des Synchronisationservers für Microsoft Teams](#) auf Seite 14
- [Synchronisationsprotokoll konfigurieren](#) auf Seite 25
- [Anpassen der Synchronisationskonfiguration für Microsoft Teams](#) auf Seite 26
- [Ausführen einer Synchronisation](#) auf Seite 34
- [Aufgaben nach einer Synchronisation](#) auf Seite 37
- [Standardprojektvorlage für Microsoft Teams](#) auf Seite 58

Synchronisationsprotokoll konfigurieren

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

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

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

Um das Synchronisationsprotokoll für die Datenbankverbindung zu konfigurieren, wählen Sie im Synchronization Editor die Kategorie **Konfiguration > One Identity Manager Verbindung**.

2. Wählen Sie den Bereich **Allgemein** und klicken Sie **Konfigurieren**.
3. Wählen Sie den Bereich **Synchronisationsprotokoll** und aktivieren Sie **Synchronisationsprotokoll erstellen**.
4. Aktivieren Sie die zu protokollierenden Daten.

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

5. Klicken Sie **OK**.

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

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

Verwandte Themen

- [Synchronisationsergebnisse anzeigen](#) auf Seite 36

Anpassen der Synchronisationskonfiguration für Microsoft Teams

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation einer Notes Domäne eingerichtet. Mit diesem Synchronisationsprojekt können Sie Microsoft Teams Objekte in die One Identity Manager-Datenbank einlesen. Änderungen werden in die Microsoft Teams-Umgebung provisioniert.

Um die Datenbank und die Microsoft Teams-Umgebung regelmäßig abzugleichen und Änderungen zu synchronisieren, passen Sie die Synchronisationskonfiguration an.

- Um bei der Synchronisation den One Identity Manager als primäres System zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um allgemeingültige Synchronisationskonfigurationen zu erstellen, die erst beim Start der Synchronisation die notwendigen Informationen über die zu synchronisierenden Objekte erhalten, können Variablen eingesetzt werden. Variablen können beispielsweise in den Basisobjekten, den Schemaklassen oder den Verarbeitungsmethoden eingesetzt werden.
- Mit Hilfe von Variablen kann ein Synchronisationsprojekt für die Synchronisation verschiedener Azure Active Directory Mandanten eingerichtet werden. Hinterlegen Sie die Verbindungsparameter zur Anmeldung an den Azure Active Directory Mandanten als Variablen.
- Um festzulegen, welche Microsoft Teams 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.
- Um zusätzliche Schemaeigenschaften zu synchronisieren, aktualisieren Sie das Schema im Synchronisationsprojekt. Nehmen Sie die Schemaerweiterungen in das Mapping auf.

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

Detaillierte Informationen zum Thema

- [Synchronisation in die Microsoft Teams-Umgebung konfigurieren](#) auf Seite 27
- [Einstellungen der Systemverbindung zur Microsoft Teams-Umgebung ändern](#) auf Seite 28
- [Schema aktualisieren](#) auf Seite 30
- [Einzelobjektsynchronisation konfigurieren](#) auf Seite 31
- [Beschleunigung der Provisionierung und Einzelobjektsynchronisation](#) auf Seite 32

Synchronisation in die Microsoft Teams-Umgebung konfigurieren

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

Um eine Synchronisationskonfiguration für die Synchronisation in die Microsoft Teams-Umgebung zu erstellen

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

Einstellungen der Systemverbindung zur Microsoft Teams-Umgebung ändern

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

- a. Legen Sie ein spezialisiertes Variablenset an und ändern Sie die Werte der betroffenen Variablen.
Die Standardwerte bleiben im Standardvariablenset erhalten. Die Variablen können jederzeit auf die Standardwerte zurückgesetzt werden. (Empfohlenes Vorgehen)
- b. Bearbeiten Sie die Zielsystemverbindung mit dem Systemverbindungsassistenten und ändern Sie die betroffenen Werte.
Der Systemverbindungsassistent liefert zusätzliche Erläuterungen zu den Einstellungen. Die Standardwerte können nur unter bestimmten Voraussetzungen wiederhergestellt werden.

Ausführliche Informationen zu den Einstellungen des Azure Active Directory Konnektors finden Sie im *<One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung>*.

Detaillierte Informationen zum Thema

- [Verbindungsparameter im Variablenset bearbeiten](#) auf Seite 28
- [Eigenschaften der Zielsystemverbindung bearbeiten](#) auf Seite 29

Verbindungsparameter im Variablenset bearbeiten

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

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

Um die Verbindungsparameter in einem spezialisierten Variablenset anzupassen

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

3. Öffnen Sie die Ansicht **Verbindungsparameter**.
Einige Verbindungsparameter können hier in Variablen umgewandelt werden. Für andere sind bereits Variablen angelegt.
4. Wählen Sie einen Parameter und klicken Sie **Umwandeln**.
5. Wählen Sie die Kategorie **Konfiguration > Variablen**.
Im unteren Bereich der Dokumentenansicht werden alle spezialisierten Variablensets angezeigt.
6. Wählen Sie ein spezialisiertes Variablenset oder klicken Sie in der Symbolleiste der Variablensetansicht .
 - Um das Variablenset umzubenennen, markieren Sie das Variablenset und klicken Sie in der Symbolleiste der Variablensetansicht . Erfassen Sie einen Namen für das Variablenset.
7. Wählen Sie die zuvor angelegten Variablen und erfassen Sie neue Werte.
8. Wählen Sie die Kategorie **Konfiguration > Startkonfigurationen**.
9. Wählen Sie eine Startkonfiguration und klicken Sie **Bearbeiten**.
10. Wählen Sie den Tabreiter **Allgemein**.
11. Ordnen Sie im Eingabefeld **Variablenset** das spezialisierte Variablenset zu.
12. Wählen Sie die Kategorie **Konfiguration > Basisobjekte**.
13. Wählen Sie ein Basisobjekt und klicken Sie .
 - ODER -
 - Klicken Sie , um ein neues Basisobjekt anzulegen.
14. Ordnen Sie im Eingabefeld **Variablenset** das spezialisierte Variablenset zu.
15. Speichern Sie die Änderungen.

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

Verwandte Themen

- [Eigenschaften der Zielsystemverbindung bearbeiten](#) auf Seite 29

Eigenschaften der Zielsystemverbindung bearbeiten

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

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

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

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

Um die Verbindungsparameter mit dem Systemverbindungsassistenten zu bearbeiten

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

HINWEIS: Ist das Standardvariablenset ausgewählt, werden die Standardwerte überschrieben und können später nicht wiederhergestellt werden.

3. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
4. Klicken Sie **Verbindung bearbeiten**.
Der Systemverbindungsassistent wird gestartet.
5. Folgen Sie den Anweisungen des Systemverbindungsassistenten und ändern Sie die gewünschten Eigenschaften.
6. Speichern Sie die Änderungen.

Verwandte Themen

- [Verbindungsparameter im Variablenset bearbeiten](#) auf Seite 28

Schema aktualisieren

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

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

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

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

Um das Schema einer Systemverbindung zu aktualisieren

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

Um ein Mapping zu bearbeiten

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

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

Einzelobjektsynchronisation konfigurieren

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

Voraussetzungen

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

Für Synchronisationsprojekte, die mit der Standard-Projektvorlage erstellt wurden, ist die Einzelobjektsynchronisation vollständig konfiguriert. Wenn Sie kundenspezifische Tabellen in solch ein Synchronisationsprojekt einbeziehen möchten, müssen Sie die Einzelobjektsynchronisation für diese Tabellen konfigurieren. Ausführliche Informationen dazu finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

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

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Exchange Online**.
3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die kundenspezifische Tabelle zu, für die Sie die Einzelobjektsynchronisation nutzen möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die kundenspezifische Tabelle und erfassen Sie den **Pfad zum Basisobjekt**.
Geben Sie den Pfad zum Basisobjekt in der ObjectWalker-Notation der VI.DB an.
Beispiel: `FK(UID_AADOrganization).XObjectKey`
8. Speichern Sie die Änderungen.

Verwandte Themen

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

Beschleunigung der Provisionierung und Einzelobjektsynchronisation

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

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

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

Um die Lastverteilung zu konfigurieren

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

Alle Jobserver müssen auf den gleichen Azure Active Directory Mandanten zugreifen können, wie der Synchronisationsserver für das jeweilige Basisobjekt.

2. Weisen Sie im Synchronization Editor an das Basisobjekt eine kundendefinierte Serverfunktion zu.

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

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

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

3. Weisen Sie diese Serverfunktion im Manager an alle Jobserver zu, welche die Prozesse zur Provisionierung und Einzelobjektsynchronisation für das Basisobjekt verarbeiten sollen.

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

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

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

Um den Synchronisationsserver ohne Lastverteilung zu nutzen

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

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

Ausführen einer Synchronisation

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

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

Detaillierte Informationen zum Thema

- [Synchronisationen starten](#) auf Seite 34
- [Synchronisation deaktivieren](#) auf Seite 35
- [Synchronisationsergebnisse anzeigen](#) auf Seite 36
- [Einzelobjekte synchronisieren](#) auf Seite 37

Synchronisationen starten

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

Um regelmäßige Synchronisationen auszuführen

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

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

Um die initiale Synchronisation manuell zu starten

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

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

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

Synchronisation deaktivieren

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

Um regelmäßige Synchronisationen zu verhindern

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
 2. Wählen Sie die Startkonfiguration und deaktivieren Sie den hinterlegten Zeitplan.
- Synchronisationen können nun nur noch manuell gestartet werden.

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

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

Um das Synchronisationsprojekt zu deaktivieren

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

Verwandte Themen

- [Erstellen eines Synchronisationsprojektes für die initiale Synchronisation mit Microsoft Teams](#) auf Seite 18

Synchronisationsergebnisse anzeigen

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

Um das Protokoll einer Synchronisation anzuzeigen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Protokolle**.
3. Klicken Sie in der Symbolleiste der Navigationsansicht ►.
In der Navigationsansicht werden die Protokolle aller abgeschlossenen Synchronisationsläufe angezeigt.
4. Wählen Sie per Maus-Doppelklick das Protokoll, das angezeigt werden soll.
Die Auswertung der Synchronisation wird als Bericht angezeigt. Sie können diesen Bericht speichern.

Um das Protokoll einer Provisionierung anzuzeigen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Protokolle**.
3. Klicken Sie in der Symbolleiste der Navigationsansicht ⚡.
In der Navigationsansicht werden die Protokolle aller abgeschlossenen Provisionierungsprozesse angezeigt.
4. Wählen Sie per Maus-Doppelklick das Protokoll, das angezeigt werden soll.
Die Auswertung der Provisionierung wird als Bericht angezeigt. Sie können diesen Bericht speichern.

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

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

Verwandte Themen

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

Einzelobjekte synchronisieren

Die Einzelobjektsynchronisation kann nur für Objekte ausgeführt werden, die in der One Identity Manager-Datenbank bereits vorhanden sind. Es werden die Änderungen an den gemappten Objekteigenschaften übernommen.

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

Um ein Einzelobjekt zu synchronisieren

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

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

Detaillierte Informationen zum Thema

- [Einzelobjektsynchronisation konfigurieren](#) auf Seite 31

Aufgaben nach einer Synchronisation

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

- [Ausstehende Objekte nachbehandeln](#) auf Seite 37
- [Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen](#) auf Seite 39

Ausstehende Objekte nachbehandeln

Objekte, die im Zielsystem nicht vorhanden sind, können bei der Synchronisation in den One Identity Manager als ausstehend gekennzeichnet werden. Damit kann verhindert

werden, dass Objekte aufgrund einer fehlerhaften Datensituation oder einer fehlerhaften Synchronisationskonfiguration gelöscht werden.

Ausstehende Objekte

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

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

Führen Sie dafür einen Zielsystemabgleich durch.

Um ausstehende Objekte nachzubearbeiten

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

In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp **Exchange Online** als Synchronisationstabellen zugewiesen sind.

2. Öffnen Sie auf dem Formular **Zielsystemabgleich**, in der Spalte **Tabelle/Objekt** den Knoten der Tabelle, für die sie ausstehende Objekte nachbearbeiten möchten.

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

- Das Synchronisationsprotokoll wurde bereits gelöscht.
- ODER -
- Im Zielsystem wurde eine Zuweisung aus einer Mitgliederliste gelöscht.
Bei der Synchronisation wird das Basisobjekt der Zuordnung aktualisiert. Dafür erscheint ein Eintrag im Synchronisationsprotokoll. Der Eintrag in der Zuordnungstabelle wird als ausstehend markiert, es gibt jedoch keinen Eintrag im Synchronisationsprotokoll.
- Im Zielsystem wurde ein Objekt gelöscht, das eine Mitgliederliste enthält.
Bei der Synchronisation werden das Objekt und alle zugehörigen Einträge in Zuordnungstabellen als ausstehend markiert. Ein Eintrag im Synchronisationsprotokoll erscheint jedoch nur für das gelöschte Objekt.

TIPP:

Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

1. Wählen Sie auf dem Formular für den Zielsystemabgleich das Objekt.
 2. Öffnen Sie das Kontextmenü und klicken Sie **Objekt anzeigen**.
3. Wählen Sie die Objekte, die Sie nachbearbeiten möchten. Mehrfachauswahl ist möglich.

4. Klicken Sie in der Formularsymbolleiste eins der folgenden Symbole, um die jeweilige Methode auszuführen.

Tabelle 6: Methoden zur Behandlung ausstehender Objekte

Symbol	Methode	Beschreibung
	Löschen	Das Objekt wird sofort in der One Identity Manager-Datenbank gelöscht. Eine Löschverzögerung wird nicht berücksichtigt. Indirekte Mitgliedschaften können nicht gelöscht werden.
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung Ausstehend wird für das Objekt entfernt. Es wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt. Voraussetzungen: <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.

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

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

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

Um die Massenverarbeitung zu deaktivieren

- Deaktivieren Sie in der Formularsymbolleiste das Symbol

HINWEIS: Damit ausstehende Objekte in der Nachbehandlung publiziert werden können, muss der Zielsystemkonnektor schreibend auf das Zielsystem zugreifen können.

Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen

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

Um kundenspezifische Tabellen in den Zielsystemabgleich aufzunehmen

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

Verwandte Themen

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

Fehleranalyse

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

- **Synchronisation simulieren**
Die Simulation ermöglicht es, das Ergebnis einer Synchronisation abzuschätzen. Dadurch können beispielsweise Fehler in der Synchronisationskonfiguration aufgedeckt werden.
- **Synchronisation analysieren**
Für die Analyse von Problemen während der Synchronisation, beispielsweise unzureichender Performance, kann der Synchronisationsanalysebericht erzeugt werden.
- **Meldungen protokollieren**
Der One Identity Manager bietet verschiedene Möglichkeiten zur Protokollierung von Meldungen. Dazu gehören das Synchronisationsprotokoll, die Protokolldatei des One Identity Manager Service, die Protokollierung von Meldungen mittels NLog und weitere.
- **Startinformation zurücksetzen**
Wenn eine Synchronisation irregulär abgebrochen wurde, beispielsweise weil ein Server nicht erreichbar war, muss die Startinformation manuell zurückgesetzt werden. Erst danach kann die Synchronisation erneut gestartet werden.

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

Verwandte Themen

- [Synchronisationsergebnisse anzeigen](#) auf Seite 36

Datenfehler bei der Synchronisation ignorieren

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

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

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

Der Systemverbindungsassistent wird gestartet.

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

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

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

5. Speichern Sie die Änderungen.

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

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

Abbildung von Microsoft Teams Objekten im One Identity Manager

Im One Identity Manager werden die Teams und Kanäle einer Microsoft Teams-Umgebung abgebildet. In einem Team werden Microsoft Teams Benutzer wie in einer Gruppe zusammengefasst. Ein Team ist mit einer Exchange Online Office 365 Gruppe verbunden. Alle Mitglieder der Office 365 Gruppe sind Mitglieder des Teams. Die Mitglieder eines Teams können die Kanäle des Teams nutzen. Standardkanäle sind für alle Mitglieder des Teams zugänglich. Private Kanäle sind nur für bestimmte Mitglieder des Teams zugänglich. Mitglieder eines Teams, die nicht in den privaten Kanal eingeladen wurden, sehen diesen Kanal nicht.

Microsoft Teams Teams und Kanäle werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Sie können einzelne Stammdaten der Teams bearbeiten und neue Teams erstellen. Sie können neue Standardkanäle erstellen. Private Kanäle können Sie nicht erstellen. Bestehende Kanäle können Sie nicht bearbeiten.

Ausführliche Informationen zu Microsoft Teams finden Sie in der *Microsoft Teams Dokumentation* von Microsoft.

Detaillierte Informationen zum Thema

- [Microsoft Teams Teams](#) auf Seite 42
- [Microsoft Teams Kanäle](#) auf Seite 50

Microsoft Teams Teams

In einem Team werden Microsoft Teams Benutzer wie in einer Gruppe zusammengefasst. Ein Team ist mit einer Exchange Online Office 365 Gruppe verbunden. Alle Mitglieder der Office 365 Gruppe sind Mitglieder des Teams.

Teams werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können einzelne Stammdaten der Teams bearbeiten und neue Teams erstellen.

Ausführliche Informationen über Exchange Online Office 365 Gruppen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung*.

Detaillierte Informationen zum Thema

- [Microsoft Teams Teams erstellen](#) auf Seite 43
- [Stammdaten für Microsoft Teams Teams bearbeiten](#) auf Seite 44
- [Microsoft Teams Teams archivieren](#) auf Seite 44
- [Microsoft Teams Teams löschen](#) auf Seite 44
- [Zuweisen von Microsoft Teams Teams an Azure Active Directory Benutzerkonten](#) auf Seite 45
- [Microsoft Teams Teams automatisch in den IT Shop aufnehmen](#) auf Seite 46
- [Mitglieder von Microsoft Teams Teams anzeigen](#) auf Seite 47
- [Eigentümer von Microsoft Teams Teams anzeigen](#) auf Seite 48
- [Überblick über Microsoft Teams Teams anzeigen](#) auf Seite 48
- [Stammdaten für Microsoft Teams Teams](#) auf Seite 49

Microsoft Teams Teams erstellen

Sie können im One Identity Manager neue Teams erstellen.

Um ein Team zu erstellen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Teams**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Tabreiter **Allgemein** wählen Sie unter **Office 365 Gruppe**, die Exchange Online Office 365 Gruppe, mit der das Team verbunden ist.
Die Mitglieder der Office 365 Gruppe werden Mitglieder des Teams. Die Eigentümer der Office 365 Gruppe werden die Eigentümer des Teams.
4. Erfassen Sie die weiteren Stammdaten des Teams.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Stammdaten für Microsoft Teams Teams bearbeiten](#) auf Seite 44
- [Stammdaten für Microsoft Teams Teams](#) auf Seite 49

Stammdaten für Microsoft Teams Teams bearbeiten

Sie können die Stammdaten bestehender Teams bearbeiten.

Um die Stammdaten eines Teams zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Teams**.
2. Wählen Sie in der Ergebnisliste das Team.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Teams.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Microsoft Teams Teams erstellen](#) auf Seite 43
- [Stammdaten für Microsoft Teams Teams](#) auf Seite 49

Microsoft Teams Teams archivieren

Sie können Teams, die nicht mehr benötigt werden, archivieren.

Um ein Team zu archivieren

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Teams**.
2. Wählen Sie in der Ergebnisliste das Team.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Auf dem Tabreiter **Allgemein** aktivieren Sie die Option **Archiviert**.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Microsoft Teams Teams löschen](#) auf Seite 44

Microsoft Teams Teams löschen

Um ein Microsoft Teams Team zu löschen, löschen Sie die Exchange Online Office 365 Gruppe, mit der das Team verbunden ist. Beim Löschen einer Office 365 Gruppe wird das Team ebenfalls gelöscht. Beim Löschen einer Office 365 Gruppe wird zusätzlich die Azure Active Directory Gruppe, die mit der Office 365 Gruppe verknüpft ist, gelöscht.

Um eine Office 365 Gruppe zu löschen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Office 365 Gruppen**.
2. Wählen Sie in der Ergebnisliste die Office 365 Gruppe.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Ausführliche Informationen über Exchange Online Office 365 Gruppen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung*.

Verwandte Themen

- [Microsoft Teams Teams archivieren](#) auf Seite 44

Zuweisen von Microsoft Teams Teams an Azure Active Directory Benutzerkonten

Teams können über ihre Office 365 Gruppe indirekt oder direkt an Azure Active Directory Benutzerkonten zugewiesen werden. Alle Mitglieder der Office 365 Gruppe sind Mitglieder des Teams.

Bei der indirekten Zuweisung werden Personen und Office 365 Gruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die Office 365 Gruppen berechnet, die einer Person zugewiesen sind. Wenn Sie eine Person in Rollen aufnehmen und die Person ein Azure Active Directory Benutzerkonto besitzt, dann wird dieses Azure Active Directory Benutzerkonto in die Office 365 Gruppen aufgenommen.

Des Weiteren können Office 365 Gruppen im Web Portal bestellt werden. Dazu werden Personen als Kunden in einen Shop aufgenommen. Alle Office 365 Gruppen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Office 365 Gruppen werden nach erfolgreicher Genehmigung den Personen zugewiesen.

Über Systemrollen können Office 365 Gruppen zusammengefasst und als Paket an Personen und Arbeitsplätze zugewiesen werden. Sie können Systemrollen erstellen, die ausschließlich Office 365 Gruppen enthalten. Ebenso können Sie in einer Systemrolle beliebige Unternehmensressourcen zusammenfassen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Office 365 Gruppen auch direkt an Azure Active Directory Benutzerkonten zuweisen.

Ausführliche Informationen über Exchange Online Office 365 Gruppen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung*.

Verwandte Themen

- [Microsoft Teams Teams automatisch in den IT Shop aufnehmen](#) auf Seite 46
- [Mitglieder von Microsoft Teams Teams anzeigen](#) auf Seite 47

Microsoft Teams Teams automatisch in den IT Shop aufnehmen

Mit den folgenden Schritten können Microsoft Teams Teams automatisch in den IT Shop aufgenommen werden. Die Synchronisation sorgt dafür, dass die Teams über ihre Office 365 Gruppen in den IT Shop aufgenommen werden.

Ausführliche Informationen über Exchange Online Office 365 Gruppen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung*.

Um Microsoft Teams Teams automatisch in den IT Shop aufzunehmen

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | O3TTeam**.
2. Um einzelne Teams nicht automatisch in den IT Shop aufzunehmen, aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | O3TTeam | ExcludeList**.

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

3. Kompilieren Sie die Datenbank.

Die Teams und ihre Office 365 Gruppen werden ab diesem Zeitpunkt automatisch in den IT Shop aufgenommen.

Folgende Schritte werden bei der Aufnahme eines Teams in den IT Shop automatisch ausgeführt.

1. Es wird eine Leistungsposition für die Office 365 Gruppe des Teams ermittelt.
2. Die Leistungsposition wird der Standard-Servicekategorie **Azure Active Directory Gruppen | Office 365 Gruppen in Microsoft Teams** zugeordnet.
3. Es wird eine Anwendungsrolle für Produkteigner ermittelt und der Leistungsposition zugeordnet.

Die Produkteigner können Bestellungen von Mitgliedschaften in diesen Teams und ihren Office 365 Gruppen genehmigen. Standardmäßig wird der Eigentümer einer Office 365 Gruppe als Produkteigner ermittelt.

4. Die Office 365 Gruppe wird mit der Option **IT Shop** gekennzeichnet und den IT Shop

Regalen **Microsoft Teams Teams** und **Office 365 Gruppen** im Shop **Identity & Access Lifecycle** zugewiesen.

Anschließend können die Kunden des Shops Mitgliedschaften in den Teams und ihren Office 365 Gruppen über das Web Portal bestellen.

HINWEIS: Wenn ein Team endgültig aus der One Identity Manager-Datenbank gelöscht wird, wird auch die zugehörige Leistungsposition gelöscht.

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

Verwandte Themen

- [Zuweisen von Microsoft Teams Teams an Azure Active Directory Benutzerkonten](#) auf Seite 45
- [Mitglieder von Microsoft Teams Teams anzeigen](#) auf Seite 47
- [Microsoft Teams Teams löschen](#) auf Seite 44

Mitglieder von Microsoft Teams Teams anzeigen

Ein Team ist mit einer Exchange Online Office 365 Gruppe verbunden. Alle Mitglieder der Office 365 Gruppe sind Mitglieder des Teams. Damit die Benutzer Microsoft Teams nutzen können, benötigen Sie einen Microsoft Teams Dienstplan. Ausführliche Informationen zu Microsoft Teams finden Sie in der *Microsoft Teams Dokumentation* von Microsoft.

Um die Mitglieder eines Teams anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Teams**.
2. Wählen Sie in der Ergebnisliste das Team.
3. Wählen Sie die Aufgabe **Überblick über das Microsoft Teams Team**.

Auf dem Überblickformular werden folgende Informationen zu den Mitgliedern eines Teams angezeigt:

- **Mitglieder:** Zeigt die Mitglieder des Teams, die einen Microsoft Teams Dienstplan besitzen. Diese Mitglieder können Microsoft Teams nutzen.
- **Mitglieder ohne den Dienstplan "Teams":** Zeigt die Mitglieder des Teams, die keinen Microsoft Teams Dienstplan besitzen. Diese Mitglieder können Microsoft Teams nicht nutzen.

Verwandte Themen

- [Überblick über Microsoft Teams Teams anzeigen](#) auf Seite 48

Eigentümer von Microsoft Teams Teams anzeigen

Ein Team ist mit einer Exchange Online Office 365 Gruppe verbunden. Die Eigentümer der Office 365 Gruppe sind die Eigentümer des Teams.

Die Eigentümer eines Teams sehen im Microsoft Teams die Kanäle eines Teams. Für private Kanäle werden nur begrenzte Informationen angezeigt. Ausführliche Informationen zu Microsoft Teams finden Sie in der *Microsoft Teams Dokumentation* von Microsoft.

Um die Eigentümer eines Teams anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Teams**.
2. Wählen Sie in der Ergebnisliste das Team.
3. Wählen Sie die Aufgabe **Überblick über das Microsoft Teams Team**.
4. Auf dem Formularelement **Office 365 Gruppen** klicken Sie im Kopfbereich auf die Gruppenbezeichnung.

Die Office 365 Gruppe des Teams wird geöffnet. Auf dem Formular **Überblick über die Office 365 Gruppe** werden die Eigentümer angezeigt.

Verwandte Themen

- [Überblick über Microsoft Teams Teams anzeigen](#) auf Seite 48
- [Microsoft Teams Kanäle](#) auf Seite 50

Überblick über Microsoft Teams Teams anzeigen

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

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Teams**.
2. Wählen Sie in der Ergebnisliste das Team.
3. Wählen Sie die Aufgabe **Überblick über das Microsoft Teams Team**.

Verwandte Themen

- [Mitglieder von Microsoft Teams Teams anzeigen](#) auf Seite 47
- [Eigentümer von Microsoft Teams Teams anzeigen](#) auf Seite 48
- [Microsoft Teams Kanäle](#) auf Seite 50

Stammdaten für Microsoft Teams Teams

Tabelle 7: Stammdaten eines Teams

Eigenschaft	Beschreibung
Office 365 Gruppe	Exchange Online Office 365 Gruppe, mit der das Team verbunden ist. Die Mitglieder der Office 365 Gruppe sind Mitglieder des Teams. Die Eigentümer der Office 365 Gruppe sind die Eigentümer des Teams. Ausführliche Informationen über Exchange Online Office 365 Gruppen finden Sie im <i>One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung</i> .
Web URL	URL, die direkt auf das Microsoft Teams Team verlinkt. Die Web URL wird durch Microsoft Teams gebildet.
Archiviert	Gibt an, ob sich das Team im schreibgeschützten Modus befindet.
Giphy zulassen	Gibt an, ob die Verwendung von Giphy erlaubt ist.
Giphy-Inhaltsklassifikation	Giphy-Inhaltsklassifikation. Mögliche Werte sind moderat und streng .
Benutzerdefinierte Memes zulassen	Gibt an, ob Benutzer benutzerdefinierte Memes einschließen können.
Sticker und Memes zulassen	Gibt an, ob Benutzer Sticker und Memes einschließen können.
Kanäle erstellen und aktualisieren (Gäste)	Gibt an, ob Gäste Kanäle erstellen und aktualisieren können.
Kanäle löschen (Gäste)	Gibt an, ob Gäste Kanäle löschen können.
Hinzufügen und Entfernen von Apps	Gibt an, ob Mitglieder Apps hinzufügen und entfernen können.
Kanäle erstellen und aktualisieren (Mitglieder)	Gibt an, ob Mitglieder Kanäle erstellen und aktualisieren können.
Kanäle löschen (Mitglieder)	Gibt an, ob Mitglieder Kanäle löschen können.
Nutzung von Konnektoren	Gibt an, ob Mitglieder Konnektoren hinzufügen, aktualisieren und entfernen können.
Nutzung von Registerkarten	Gibt an, ob Mitglieder Registerkarten hinzufügen, aktualisieren und entfernen können.

Eigenschaft	Beschreibung
Nachrichten bearbeiten zulassen (Benutzer)	Gibt an, ob Benutzer ihre Nachrichten bearbeiten können.
Nachrichten löschen zulassen (Benutzer)	Gibt an, ob Benutzer ihre Nachrichten löschen können.
Nachrichten löschen zulassen (Eigentümer)	Gibt an, ob Eigentümer alle Nachrichten löschen dürfen.
Erwähnung des Kanals zulassen	Gibt an, ob Erwähnungen des Kanals (@Channel) zulässig sind.
Erwähnung des Teams zulassen	Gibt an, ob Erwähnungen des Teams (@Team) zulässig sind.

Verwandte Themen

- [Stammdaten für Microsoft Teams Teams bearbeiten](#) auf Seite 44
- [Microsoft Teams Teams archivieren](#) auf Seite 44
- [Mitglieder von Microsoft Teams Teams anzeigen](#) auf Seite 47
- [Eigentümer von Microsoft Teams Teams anzeigen](#) auf Seite 48

Microsoft Teams Kanäle

Ein Team ist mit einer Exchange Online Office 365 Gruppe verbunden. Alle Mitglieder der Office 365 Gruppe sind Mitglieder des Teams. Die Mitglieder eines Teams können die Kanäle des Teams nutzen. Standardkanäle sind für alle Mitglieder des Teams zugänglich. Private Kanäle sind nur für bestimmte Mitglieder des Teams zugänglich. Mitglieder eines Teams, die nicht in den privaten Kanal eingeladen wurden, sehen diesen Kanal nicht.

Kanäle werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können neue Standardkanäle erstellen. Private Kanäle können Sie nicht erstellen. Bestehende Kanäle können Sie nicht bearbeiten.

Detaillierte Informationen zum Thema

- [Microsoft Teams Standardkanäle erstellen](#) auf Seite 51
- [Private Microsoft Teams Kanäle anzeigen](#) auf Seite 51
- [Microsoft Teams Kanäle löschen](#) auf Seite 52
- [Überblick über Microsoft Teams Kanäle anzeigen](#) auf Seite 53
- [Stammdaten für Microsoft Teams Kanäle](#) auf Seite 53

- [Mitglieder von Microsoft Teams Teams anzeigen](#) auf Seite 47
- [Eigentümer von Microsoft Teams Teams anzeigen](#) auf Seite 48

Microsoft Teams Standardkanäle erstellen

Sie können im One Identity Manager neue Standardkanäle erstellen. Private Kanäle können Sie im One Identity Manager nicht erstellen.

Um einen Standardkanal zu erstellen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Kanäle**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Tabreiter Allgemein erfassen Sie folgende Informationen:
 - **Anzeigename:** Kanalname, der in Microsoft Teams für die Benutzer angezeigt wird.
 - **Mitgliedschaftstyp:** Standardkanäle werden mit dem Wert **Standard** erstellt. Der Kanal ist für alle Mitglieder des Teams zugänglich.
 - **Beschreibung:** Nähere Beschreibung für den Kanal.
 - **Team:** Wählen Sie das Team, zu dem der Kanal gehört.
4. Speichern Sie die Änderungen.

Verwandte Themen

- [Private Microsoft Teams Kanäle anzeigen](#) auf Seite 51
- [Stammdaten für Microsoft Teams Kanäle](#) auf Seite 53
- [Mitglieder von Microsoft Teams Teams anzeigen](#) auf Seite 47

Private Microsoft Teams Kanäle anzeigen

Private Kanäle können Sie im One Identity Manager nicht erstellen. Sie können die Stammdaten und die Eigentümer der privaten Kanäle anzeigen. Die Mitglieder werden im One Identity Manager nicht angezeigt.

Um die Stammdaten eines privaten Kanals anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Kanäle**.
2. Wählen Sie in der Ergebnisliste den Kanal.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Auf dem Tabreiter Allgemein werden folgenden Informationen angezeigt.

- **Anzeigename:** Kanalname, der in Microsoft Teams für die Benutzer angezeigt wird.
- **Mitgliedschaftstyp:** Für private Kanäle wird der Wert **Privat** angezeigt. Der Kanal ist nur für bestimmte Mitglieder des Teams zugänglich.
- **Beschreibung:** Nähere Beschreibung für den Kanal.
- **Team:** Wählen Sie das Team, zu dem der Kanal gehört.

Um die Eigentümer eines privaten Kanals anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Kanäle**.
2. Wählen Sie in der Ergebnisliste den Kanal.
3. Wählen Sie die Aufgabe **Überblick über den Microsoft Teams Kanal**.

Das Formularelement **Microsoft Teams Kanaleigentümer** zeigt die Eigentümer des privaten Kanals.

Verwandte Themen

- [Überblick über Microsoft Teams Kanäle anzeigen](#) auf Seite 53
- [Microsoft Teams Standardkanäle erstellen](#) auf Seite 51
- [Stammdaten für Microsoft Teams Kanäle](#) auf Seite 53

Microsoft Teams Kanäle löschen

Der Kanal wird endgültig aus der One Identity Manager-Datenbank und der Microsoft Teams-Umgebung gelöscht.

HINWEIS: Kanäle mit der Bezeichnung **General** können im One Identity Manager nicht gelöscht werden.

Um einen Kanal zu löschen

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

Verwandte Themen

- [Bekannte Probleme bei der Anbindung von Microsoft Teams](#) auf Seite 60

Überblick über Microsoft Teams Kanäle anzeigen

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

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Kanäle**.
2. Wählen Sie in der Ergebnisliste den Kanal.
3. Wählen Sie die Aufgabe **Überblick über den Microsoft Teams Kanal**.

Verwandte Themen

- [Private Microsoft Teams Kanäle anzeigen](#) auf Seite 51

Stammdaten für Microsoft Teams Kanäle

Tabelle 8: Stammdaten eines Kanals

Eigenschaft	Beschreibung
Anzeigename	Kanalname, der in Microsoft Teams für die Benutzer angezeigt wird.
Beschreibung	Nähere Beschreibung des Kanals
Team	Teams, zu dem der Kanal gehört.
E-Mail-Adresse	E-Mail-Adresse zum Senden von Nachrichten an den Kanal. Die E-Mail-Adresse wird durch Microsoft Teams gebildet.
Web URL	URL, die direkt auf den Microsoft Teams Kanal verlinkt. Die Web URL wird durch Microsoft Teams gebildet.
Mitgliedschaftstyp	Typ des Kanals. Zur Auswahl stehen: <ul style="list-style-type: none">• Standard: Es handelt sich um einen Standardkanal. Der Kanal ist für alle Mitglieder des Teams zugänglich.• Privat: Es handelt sich um einen privaten Kanal. Der Kanal ist nur für bestimmte Mitglieder des Teams zugänglich.

Basisdaten für die Verwaltung einer Microsoft Teams-Umgebung

Für die Verwaltung einer Microsoft Teams-Umgebung im One Identity Manager sind folgende Basisdaten relevant.

- Zielsystemtypen

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

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

- Zielsystemverantwortliche

Die Zielsystemverantwortlichen für Exchange Online sind ebenfalls für die Microsoft Teams-Objekte verantwortlich. Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Exchange Online** oder einer untergeordneten Anwendungsrolle zugewiesen sein.

Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung*.

- Server

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

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

- Konfigurationsparameter

Über Konfigurationsparameter konfigurieren Sie die Grundeinstellungen zum Systemverhalten. Der One Identity Manager stellt für verschiedene

Konfigurationsparameter Standardeinstellungen zur Verfügung. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.

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

Weitere Informationen finden Sie unter [Konfigurationsparameter für die Verwaltung einer Microsoft Teams-Umgebung](#) auf Seite 56.

Konfigurationsparameter für die Verwaltung einer Microsoft Teams-Umgebung

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

Tabelle 9: Konfigurationsparameter

Konfigurationsparameter	Beschreibung
TargetSystem AzureAD ExchangeOnline Teams	<p>Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung des Zielsystems Microsoft Teams. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.</p> <p>Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im <i>One Identity Manager Konfigurationshandbuch</i>.</p>
QER ITShop AutoPublish O3TTeam	<p>Präprozessorrelevanter Konfigurationsparameter zur Steuerung der automatischen Übernahme von Microsoft Teams Teams in den IT Shop. Ist der Parameter aktiviert, werden alle Teams automatisch als Produkte dem IT Shop zugewiesen. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.</p> <p>Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und</p>

Konfigurationsparameter	Beschreibung
-------------------------	--------------

	Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im <i>One Identity Manager Konfigurationshandbuch</i> .
--	--

QER ITShop AutoPublish O3TTeam ExcludeList	Auflistung aller Microsoft Teams Teams, für die keine automatische Zuordnung zum IT Shop erfolgen soll. Jeder Eintrag ist Bestandteil eines regulären Suchmusters und unterstützt die Notation für reguläre Ausdrücke.
--	--

Standardprojektvorlage für Microsoft Teams

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

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

Die Projektvorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 10: Abbildung der Microsoft Teams Schematypen

Schematyp im Microsoft Teams	Tabelle im One Identity Manager Schema
Channel	O3TTeamChannel
Team	O3TTeam

Verarbeitung von Microsoft Teams Systemobjekten

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

Tabelle 11: Zulässige Verarbeitungsmethoden für Schematypen

Typ	Lesen	Hinzufügen	Löschen	Aktualisieren
Teams (Team)	Ja	Ja	Nein	Ja
Standardkanäle (Channel)	Ja	Ja	Ja	Nein
Private Kanäle (Channel)	Ja	Nein	Nein	Nein

Bekannte Probleme bei der Anbindung von Microsoft Teams

Problem

Beim Erstellen eines Kanals tritt eine Fehlermeldung auf: Kanalname bereits vergeben.

Ursache

Wurde in Microsoft Teams ein Kanal erstellt und gelöscht, ist es nicht möglich einen Kanal unter dem selben Namen neu zu erstellen.

Lösung

Keine.

Dieses Verhalten ist Standardverhalten von Microsoft Teams. Ausführliche Informationen zu Microsoft Teams finden Sie in der *Microsoft Teams Dokumentation* von Microsoft.

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

A

- Architekturüberblick 6
- Ausstehendes Objekt 37
- Azure Active Directory
 - Anwendung 12
- Azure Active Directory Konnektor 15

B

- Basisobjekt 28, 31

E

- Einzelobjekt synchronisieren 37
- Einzelobjektsynchronisation 31, 37
 - beschleunigen 32
- Exchange Online Organisation
 - Anwendungsrollen 7
 - Zielsystemverantwortlicher 7, 54

J

- Jobserver
 - bearbeiten 14
 - Lastverteilung 32

K

- Konfigurationsparameter 56

L

- Lastverteilung 32

M

- Microsoft Teams
 - Zielsystemverantwortlicher 7, 54
- Microsoft Teams Kanal 50
 - erstellen 51
 - löschen 52
 - Standardkanal 51
 - Team 53
- Microsoft Teams Team 42
 - archivieren 44
 - bearbeiten 44
 - Eigentümer 48
 - erstellen 43
 - in IT Shop aufnehmen 46
 - löschen 44
 - Mitglieder 47
 - Office 365 Gruppe 49

O

- Objekt
 - ausstehend 37
 - publizieren 37
 - sofort löschen 37
- One Identity Manager
 - als Anwendung registrieren 12

P

- Projektvorlage 58

Provisionierung
beschleunigen 32

S

Schema

aktualisieren 30
Änderungen 30
komprimieren 30

Startkonfiguration 28

Synchronisation

Benutzer 13
Berechtigungen 13
einrichten 10
konfigurieren 18, 26
Scope 26
starten 18, 34
Synchronisationsprojekt
erstellen 18
Variable 26
Verbindungsparameter 18, 26
verhindern 35
Workflow 18, 27
Zeitplan 34

Synchronisationskonfiguration

anpassen 26-27

Synchronisationsprojekt

deaktivieren 35
erstellen 18
Projektvorlage 58

Synchronisationsprotokoll 36

erstellen 25
Inhalt 25

Synchronisationsrichtung

In das Zielsystem 18, 27
In den Manager 18

Synchronisationsserver

installieren 14
Jobserver 14
konfigurieren 14

Synchronisationsworkflow

erstellen 18, 27

Systemverbindung

aktives Variablenset 29
ändern 28

V

Variablenset 28

aktiv 29

Verbindungsparameter umwandeln 28

Z

Zeitplan 34

deaktivieren 35

Zielsystemabgleich 37