One Identity Manager 8.1.4

Administrationshandbuch für die Anbindung einer G Suite-Umgebung

Legende

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

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

One Identity Manager Administrationshandbuch für die Anbindung einer G Suite-Umgebung
Aktualisiert - 19. Oktober 2020, 08:14 Uhr
Version - 8.1.4

Inhalt

1

Abbilden einer G Suite im One Identity Manager

Der One Identity Manager bietet eine vereinfachte Administration der Nutzer einer G Suite. Dabei konzentriert sich der One Identity Manager auf die Einrichtung und Bearbeitung von Benutzerkonten und die Versorgung mit den benötigten Berechtigungen. Dafür werden Gruppen, Organisationen, Berechtigungen, Admin-Rollen, Produkte und SKUs im One Identity Manager abgebildet.

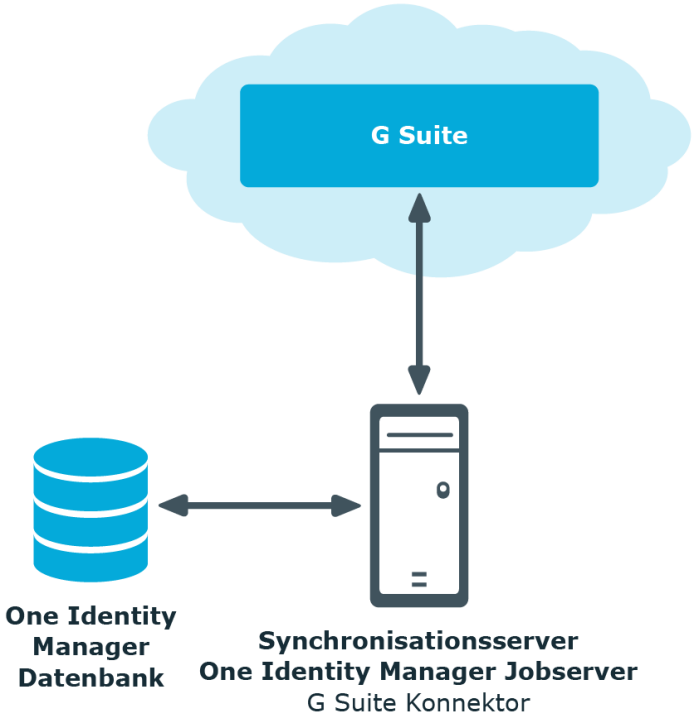
Im One Identity Manager werden die Personen eines Unternehmens mit den benötigten Benutzerkonten versorgt. Dabei können Sie unterschiedliche Mechanismen für die Verbindung der Personen mit ihren Benutzerkonten nutzen. Ebenso können Sie die Benutzerkonten getrennt von Personen verwalten und somit administrative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

Ausführliche Informationen zur G Suite Struktur finden Sie in der G Suite Dokumentation von Google Inc.

Architekturüberblick

Um auf die Daten einer G Suite zuzugreifen, wird auf einem Synchronisationsserver der G Suite Konnektor installiert. Der G Suite Konnektor stellt die Kommunikation mit der zu synchronisierenden G Suite, über mehrere von Google Inc. bereitgestellte REST APIs her. Der Synchronisationsserver sorgt für den Abgleich der Daten zwischen der One Identity Manager-Datenbank und der G Suite.

Abbildung 1: Architektur für die Synchronisation



One Identity Manager Benutzer für die Verwaltung einer G Suite

In die Einrichtung und Verwaltung einer G Suite sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

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

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

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

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 G Suite auf Seite 172.

2

Synchronisieren einer G Suite

Der One Identity Manager unterstützt die Synchronisation mit einer G Suite. Für den Abgleich der Informationen zwischen der One Identity Manager-Datenbank und der G Suite sorgt der One Identity Manager Service.

Informieren Sie sich hier:

- wie Sie die Synchronisation einrichten, um initial Daten aus einer G Suite in die One Identity Manager-Datenbank einzulesen,
- wie Sie eine Synchronisationskonfiguration anpassen, beispielsweise um verschiedene Kunden-Umgebungen mit ein und demselben Synchronisationsprojekt zu synchronisieren,
- wie Sie die Synchronisation starten und deaktivieren,
- wie Sie die Synchronisationsergebnisse auswerten.

TIPP: Bevor Sie die Synchronisation mit einer G Suite 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 einer G Suite auf Seite 14
- Anpassen der Synchronisationskonfiguration für G Suite-Umgebungen auf Seite 28
- Ausführen einer Synchronisation auf Seite 41
- Fehleranalyse auf Seite 49
- Verarbeitung von Systemobjekten einer G Suite auf Seite 179

Einrichten der Initialsynchronisation einer G Suite

Der Synchronization Editor stellt eine Projektvorlagen bereit, mit der die Synchronisation von Benutzerkonten und Berechtigungen der G Suite eingerichtet werden kann. Nutzen Sie diese Projektvorlagen, um Synchronisationsprojekte zu erstellen, mit denen Sie Daten aus einer G Suite 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.

Um die Objekte einer G Suite initial in die One Identity Manager Datenbank einzulesen

1. Stellen Sie in der G Suite einen Benutzer für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Die One Identity Manager Bestandteile für die Verwaltung von G Suite-Umgebungen sind verfügbar, wenn der Konfigurationsparameter **TargetSystem | GoogleApps** aktiviert ist.
    - Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.
    - Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.
3. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
4. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Detaillierte Informationen zum Thema

- Benutzer und Berechtigungen für die Synchronisation mit einer G Suite auf Seite 15
- Systemanforderungen für den G Suite Synchronisationsservers auf Seite 18
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer G Suite auf Seite 21
- Konfigurationsparameter für die Verwaltung einer G Suite auf Seite 172
- Standardprojektvorlage für eine G Suite auf Seite 175

Benutzer und Berechtigungen für die Synchronisation mit einer G Suite

Bei der Synchronisation des One Identity Manager mit einer G Suite spielen folgende Benutzer eine Rolle.

Tabelle 2: Benutzer für die Synchronisation

Benutzer	Berechtigungen
Benutzer für den Zugriff auf das Zielsystem (Synchronisationsbenutzer)	Für eine vollständige Synchronisation von Objekten einer G Suite mit der ausgelieferten One Identity Manager Standardkonfiguration stellen Sie mindestens einen Nutzer mit Super Admin Berechtigungen und ein Dienstkonto zur Authentifizierung bereit. • Das Google Cloud Platform Projekt benötigt Zugriff auf folgende APIs: Admin SDK Enterprise License Manager API Groups Settings API • Zur Authentifizierung wird ein Dienstkonto mit der zugehörigen JSON-Schlüsseldatei und domain-übergreifender G Suite-Delegation benötigt. • In der Google Admin-Konsole muss der API-Zugriff aktiviert sein. • In der Google Admin-Konsole muss die Client-ID des Dienstkontos auf verschiedene API-Bereiche autorisiert werden. Eine Liste der API-Bereiche finden Sie auf dem One Identity Manager-Installationsmedium. Diese Liste kann als Kopiervorlage genutzt werden. Verzeichnis: `Modules\GAP\dvd\AddOn\ApiAccess` Datei: `GSuiteRequiredAPIAccess.txt` Weitere Informationen finden Sie unter Einrichten der erforderlichen Berechtigungen für den Zugriff auf die G Suite auf Seite 16.
Benutzerkonto des One Identity Manager Service	Das Benutzerkonto für den One Identity Manager Service benötigt die Rechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Rechte vergeben, Verzeichnisse und Dateien anlegen und bearbeiten. Das Benutzerkonto muss der Gruppe **Domänen-Benutzer** angehören.

Benutzer	Berechtigungen
	Das Benutzerkonto benötigt das erweiterte Benutzerrecht **Anmelden als Dienst**. Das Benutzerkonto benötigt Rechte für den internen Webservice. HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so können Sie die Rechte für den internen Webservice über folgenden Kommandozeilenaufruf vergeben: `netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"` Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis. In der Standardinstallation wird der One Identity Manager installiert unter: • `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen) • `%ProgramFiles%\One Identity` (auf 64-Bit Betriebssystemen)
Benutzer für den Zugriff auf die One Identity Manager-Datenbank	Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer **Synchronization** bereitgestellt.

Verwandte Themen

- API-Bereiche für das Dienstkonto auf Seite 177
- Erweiterte Einstellungen der Systemverbindung zur G Suite auf Seite 32

Einrichten der erforderlichen Berechtigungen für den Zugriff auf die G Suite

Damit der G Suite Konnektor auf das Zielsystem zugreifen kann, müssen die erforderlichen Berechtigungen in zwei Google Webfrontends eingerichtet werden.

Um das Dienstkonto zu erstellen und APIs zu aktivieren

1. Öffnen Sie die Google Cloud Platform-Konsole (https://console.cloud.google.com).
2. Melden Sie sich als Super Admin der G Suite an.

3. Wählen Sie ein Projekt aus oder erstellen Sie ein neues Projekt.
4. Aktivieren Sie die APIs **Admin SDK**, **Enterprise License Manager API** und **Groups Settings API**.
5. Erstellen Sie ein Dienstkonto.

   Tabelle 3: Eigenschaften des Dienstkontos

Eigenschaft	Wert
Rolle	
Neuen privaten Schlüssel bereitstellen	aktiviert
Schlüsseltyp	JSON
Domainübergreifende G Suite-Delegation aktivieren	aktiviert

6. Notieren Sie sich die Client-ID des Dienstkontos.

   Sie wird beim Einrichten der API-Berechtigungen benötigt.
7. Speichern Sie die Schlüsseldatei lokal.

   Sie wird beim Erstellen des Synchronisationsprojekts benötigt.

Um den API-Zugriff zu aktivieren und die Client-ID des Dienstkontos auf die benötigten API-Bereiche zu autorisieren

1. Öffnen Sie die Google Admin-Konsole (https://admin.google.com).
2. Melden Sie sich als Super Admin der G Suite an.
3. Aktivieren Sie den API-Zugriff.
4. Autorisieren Sie die Client-ID des Dienstkontos auf die benötigten API-Bereiche.

   Weitere Informationen finden Sie unter Benutzer für den Zugriff auf das Zielsystem (Synchronisationsbenutzer) auf Seite 15.
5. Richten Sie bei Bedarf weitere Nutzer mit Super Admin Berechtigungen ein.

   Es können bis zu acht Nutzer mit Super Admin Berechtigungen für die Synchronisation genutzt werden. Jeder Nutzer muss sich mindestens einmal an der G Suite angemeldet und die Nutzungsbedingungen akzeptiert haben.

Einrichten des G Suite Synchronisationsservers

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

Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem G Suite Konnektor installiert werden.

Detaillierte Informationen zum Thema

- Systemanforderungen für den G Suite Synchronisationsservers auf Seite 18
- One Identity Manager Service installieren auf Seite 18

Systemanforderungen für den G Suite Synchronisationsservers

Für die Einrichtung der Synchronisation mit einer G Suite muss ein Server zur Verfügung gestellt werden, auf dem die nachfolgend genannte Software installiert ist:

- Windows Betriebssystem

  Unterstützt werden die Versionen:

  - Windows Server 2008 R2 (nicht-Itanium 64-Bit) ab Service Pack 1
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
- Microsoft .NET Framework Version 4.7.2 oder höher

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.

One Identity Manager Service installieren

Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem G Suite Konnektor installiert sein. Außerdem muss der Synchronisationsserver im One Identity Manager als Jobserver bekannt sein.

Tabelle 4: Eigenschaften des Jobservers

Eigenschaft	Wert
Serverfunktion	G Suite Konnektor
Maschinenrolle	Server | Jobserver | G Suite

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

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

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

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

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

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

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

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

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

       - ODER -

       Um einen neuen Jobserver zur erstellen, klicken Sie **Hinzufügen**.
    b. Bearbeiten Sie folgende Informationen für den Jobserver.
        - **Server**: Bezeichnung des Jobservers.
        - **Queue**: Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes

muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.

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

  Syntax:

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

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

4. Auf der Seite **Maschinenrollen** wählen Sie **G Suite**.
5. Auf der Seite **Serverfunktionen** wählen Sie **G Suite Konnektor**.
6. Auf der Seite **Dienstkonfiguration** erfassen Sie die Verbindungsinformationen und prüfen Sie die Konfiguration des One Identity Manager Service.

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

   - Für eine direkte Verbindung zu Datenbank:
     a. Wählen Sie **Prozessabholung | sqlprovider**
     b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     c. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
   - Für eine Verbindung zum Anwendungsserver:
     a. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
     b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     c. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.
     d. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
     e. Wählen Sie das Authentifizierungsmodul. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
7. Zur Konfiguration der Remote-Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

9. Auf der Seite **Installationsquelle festlegen** wählen Sie das Verzeichnis mit den Installationsdateien.
10. Auf der Seite **Datenbankschlüsseldatei auswählen** wählen die Datei mit dem privaten Schlüssel.

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

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

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

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer G Suite

Verwenden Sie den Synchronization Editor, um die Synchronisation zwischen One Identity Manager-Datenbank und G Suite 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.

Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

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

Tabelle 5: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Primäre Domain	Name der primären Domain der G Suite.
Schlüsseldatei des Dienstkontos	JSON-Schlüsseldatei, die beim Einrichten des Dienstkontos gespeichert wurde.
Super Admin-E-Mail-Adressen zur Anmeldung	Es können bis zu acht Super Admins angegeben werden, die zum Synchronisieren der G Suite genutzt werden. Je mehr angegeben werden, umso stärker können Zugriffe parallelisiert werden. Die Gesamtlaufzeit der Anfragen kann sich verbessern. Stellen Sie mindestens einen Nutzer mit Super Admin Berechtigungen bereit. Weitere Informationen finden Sie unter Benutzer und Berechtigungen für die Synchronisation mit einer G Suite auf Seite 15.
Synchronisationsserver für die G Suite	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 G Suite Konnektor installiert sein. **Tabelle 6: Zusätzliche Eigenschaften für den Jobserver** Eigenschaft: Wert Serverfunktion: G Suite Konnektor Maschinenrolle: Server/Jobserver/G Suite

Angaben	Erläuterungen
	Weitere Informationen finden Sie unter Systemanforderungen für den G Suite Synchronisationsservers auf Seite 18.
Verbindungsdaten zur One Identity Manager-Datenbank	• Datenbankserver • Datenbank • SQL Server Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
Remoteverbindungsserver	Um die Synchronisation mit einem Zielsystem zu konfigurieren, muss der One Identity Manager Daten aus dem Zielsystem auslesen. Dabei kommuniziert der One Identity Manager direkt mit dem Zielsystem. Mitunter ist der direkte Zugriff von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, nicht möglich, beispielsweise aufgrund der Firewall-Konfiguration oder weil die Arbeitsstation nicht die notwendigen Hard- oder Softwarevoraussetzungen erfüllt. Wenn der direkte Zugriff von der Arbeitsstation nicht möglich ist, kann eine Remoteverbindung eingerichtet werden. Der Remoteverbindungsserver und die Arbeitsstation müssen in der selben Active Directory Domäne stehen. Konfiguration des Remoteverbindungsservers: • One Identity Manager Service ist gestartet • **RemoteConnectPlugin** ist installiert • G Suite 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*.

Initiales Synchronisationsprojekt für eine G Suite 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.

Um ein initiales Synchronisationsprojekt für eine G Suite einzurichten

1. Starten Sie das Launchpadund melden Sie sich an der One Identity Manager-Datenbank an.

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

2. Wählen Sie den Eintrag **Zielsystemtyp G Suite** 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 **Primäre Domain und Dienstkonto** geben Sie die primäre Domain des G Suite-Kontos sowie die Schlüsseldatei des Dienstkontos an.

Tabelle 7: Anmeldeinformationen für die Verbindung zur G Suite

Eigenschaft	Beschreibung
Primäre Domain	Name der primären Domain der G Suite.
Schlüsseldatei des Dienstkontos	JSON-Schlüsseldatei, die beim Einrichten des Dienstkontos gespeichert wurde.

Eigenschaft	Beschreibung
	• Ziehen Sie die Schlüsseldatei per Drag and Drop in das Eingabefeld, um sie zu laden. - ODER - • Klicken Sie **Schlüsseldatei öffnen** und wählen Sie den Pfad zur Schlüsseldatei.

5. Auf der Seite **G Suite Administratoren** geben Sie die E-Mail-Adressen aller Super Admins an, die der G Suite Konnektor zur Anmeldung am Zielsystem nutzen kann.

   Es können bis zu acht Super Admins angegeben werden. Je mehr angegeben werden, umso stärker können Zugriffe parallelisiert werden. Die Gesamtlaufzeit der Anfragen kann sich verbessern.

   - Klicken Sie **Verbindung testen**, um die Verbindungsdaten zu prüfen.

     Es werden alle Administratorkonten auf Gültigkeit geprüft und, ob die korrekten API-Bereiche autorisiert sind.

6. Auf der Seite **Lokaler Cache** legen Sie fest, ob der lokale Cache des G Suite Konnektors genutzt werden soll. Bei einer Vollsynchronisation werden dadurch die Zugriffe auf die G Suite minimiert. Es wird vermieden, dass durch die Synchronisation die API-Kontingente überschritten werden.

   Die Option ist standardmäßig aktiviert. Sie sollte nur für Fehleranalysen deaktiviert werden.

7. 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**.

8. Auf der Seite **One Identity Manager Verbindung** überprüfen Sie die Verbindungsdaten zur One Identity Manager-Datenbank. Die Daten werden aus der verbundenen Datenbank geladen. Geben Sie das Kennwort erneut ein.

   HINWEIS: Wenn Sie mit einer unverschlüsselten One Identity Manager-Datenbank arbeiten und noch kein Synchronisationsprojekt in der Datenbank gespeichert ist, erfassen Sie alle Verbindungsdaten neu. Wenn bereits ein Synchronisationsprojekt gespeichert ist, wird diese Seite nicht angezeigt.

9. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.

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

Tabelle 8: Zielsystemzugriff festlegen

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

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.

    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**.

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

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

Verwandte Themen

- Synchronisationsprotokoll konfigurieren auf Seite 27
- Anpassen der Synchronisationskonfiguration für G Suite-Umgebungen auf Seite 28
- Standardprojektvorlage für eine G Suite auf Seite 175
- API-Bereiche für das Dienstkonto auf Seite 177

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 43

Anpassen der Synchronisationskonfiguration für G Suite-Umgebungen

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation einer Kunden-Umgebung eingerichtet. Mit diesem Synchronisationsprojekt können Sie G Suite Objekte in die One Identity Manager-Datenbank einlesen. Wenn Sie Benutzerkonten und ihre Berechtigungen mit dem One Identity Manager verwalten, werden Änderungen in die G Suite provisioniert.

HINWEIS: Wenn die Konfiguration von bereits bestehenden Synchronisationsprojekten angepasst werden soll, prüfen Sie, welche Auswirkungen die Änderungen auf die bereits synchronisierten Daten haben können.

Um die Datenbank und die G Suite regelmäßig abzugleichen und Änderungen zu synchronisieren, passen Sie die Synchronisationskonfiguration an.

- Um bei der Synchronisation den One Identity Manager als Mastersystem zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um festzulegen, welche G Suite 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.
- 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 Kunden-Umgebungen eingerichtet werden. Hinterlegen Sie die Verbindungsparameter zur Anmeldung an der jeweiligen G Suite als Variablen.
- Wenn sich das One Identity Manager Schema oder das Zielsystemschema geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.
- Um zusätzliche Schemaeigenschaften zu synchronisieren, aktualisieren Sie das Schema im Synchronisationsprojekt. Nehmen Sie die Schemaerweiterungen in das Mapping auf.
- Um Daten zu synchronisieren, für die keine Schematypen im Konnektorschema angelegt sind, legen Sie eigene Schematypen an. 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 G Suite konfigurieren auf Seite 29
- Synchronisation verschiedener Kunden-Umgebungen konfigurieren auf Seite 30
- Schema aktualisieren auf Seite 31
- Erweiterte Einstellungen der Systemverbindung zur G Suite auf Seite 32

Synchronisation in die G Suite konfigurieren

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

Um eine Synchronisationskonfiguration für die Synchronisation in die G Suite zu erstellen

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

   Es wird ein Workflow mit der Synchronisationsrichtung **In das Zielsystem** angelegt.

4. Erstellen Sie eine neue Startkonfiguration. Nutzen Sie dabei den neu angelegten Workflow.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

Verwandte Themen

- Synchronisation verschiedener Kunden-Umgebungen konfigurieren auf Seite 30

Synchronisation verschiedener Kunden-Umgebungen konfigurieren

Unter bestimmten Voraussetzungen ist es möglich ein Synchronisationsprojekt für die Synchronisation verschiedener Kunden-Umgebungen zu nutzen.

Voraussetzungen

- Die Zielsystemschemas der Kunden-Umgebungen sind identisch.
- Alle virtuellen Schemaeigenschaften, die im Mapping genutzt werden, müssen in den erweiterten Schemas der Kunden-Umgebungen vorhanden sein.
- Die Verbindungsparameter zum Zielsystem sind als Variablen hinterlegt.

Um ein Synchronisationsprojekt für die Synchronisation einer weiteren Kunden-Umgebung anzupassen

1. Stellen Sie in der weiteren Kunden-Umgebung einen Benutzer für den Zugriff auf die G Suite mit ausreichenden Berechtigungen bereit.
2. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
3. Erstellen Sie für die weitere Kunden-Umgebung ein neues Basisobjekt. Verwenden Sie den Assistenten zur Anlage eines Basisobjektes.
    - Wählen Sie im Assistenten den G Suite Konnektor und geben Sie die Verbindungsparameter bekannt. Die Verbindungsparameter werden in einem spezialisierten Variablenset gespeichert.

      Es wird eine Startkonfiguration erstellt, die das neu angelegte Variablenset verwendet.
4. Passen Sie bei Bedarf weitere Komponenten der Synchronisationskonfiguration an.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

Verwandte Themen

- Synchronisation in die G Suite konfigurieren auf Seite 29

Schema aktualisieren

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

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

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

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

Um das Schema einer Systemverbindung zu aktualisieren

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

   - ODER -

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

   Die Schemadaten werden neu geladen.

Um ein Mapping zu bearbeiten

1. Wählen Sie die Kategorie **Mappings**.
2. Wählen Sie in der Navigationsansicht das Mapping.

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

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

Beschleunigung der Synchronisation durch Revisionsfilterung

Die Synchronisation mit einer G Suite unterstützt keine Revisionsfilterung.

Erweiterte Einstellungen der Systemverbindung zur G Suite

An der Zielsystemverbindung können verschiedene zusätzliche Einstellungen vorgenommen werden, beispielsweise um die Anzahl an Wiederholversuchen oder Wartezeiten festzulegen. Beim Einrichten der initialen Synchronisation werden für diese Eigenschaften der Systemverbindung Standardwerte gesetzt. Diese Standardwerte können angepasst werden, beispielsweise um die Analyse von Synchronisationsproblemen zu unterstützen.

Um die Standardwerte zu ändern, 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.

   Weitere Informationen finden Sie unter Verbindungsparameter im Variablenset bearbeiten auf Seite 35.

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.

   Weitere Informationen finden Sie unter Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 36.

HINWEIS: Wenn der Projektassistent beim initialen Einrichten der Synchronisation direkt aus dem Synchronization Editor gestartet wird, können Sie die erweiterten Einstellungen bereits beim Einrichten des Synchronisationsprojekts bearbeiten. In diesem Fall werden die Standardwerte sofort durch Ihre Einstellungen überschrieben.

Tabelle 9: Erweiterte Einstellungen der Zielsystemverbindung

Eigenschaft	Beschreibung
Nur lesender API-Zugriff	Gibt an, ob die API-Bereiche für den Nur-Lese-Zugriff in der Google Admin-Konsole eingetragen wurden. Aktivieren Sie diese Option, wenn auf das Zielsystem keinerlei schreibende Berechtigung vergeben werden darf. Der Konnektor kann dann ausschließlich lesend auf das Zielsystem zugreifen. • In der Google Admin-Konsole muss die Client-ID des Dienstkontos auf verschiedene API-Bereiche autorisiert werden. Eine Liste der API-Bereiche finden Sie auf dem One Identity Manager-Installationsmedium. Diese Liste kann als Kopiervorlage genutzt werden. Verzeichnis: `Modules\GAP\dvd\AddOn\ApiAccess` Datei: `GSuiteRequiredAPIAccessReadOnly.txt` Wenn die Option deaktiviert ist, sind Lese- und Schreibzugriffe möglich. Dafür müssen andere API-Bereiche autorisiert werden.
Lokalen Cache verwenden	Angabe, ob der lokale Cache des G Suite Konnektors genutzt werden soll. Der lokale Cache wird genutzt, um zu vermeiden, dass durch die Synchronisation die API-Kontingente überschritten werden. Bei einer Vollsynchronisation werden die Zugriffe auf die G Suite minimiert. Bei der Provisionierung wird die Option ignoriert. Die Option ist standardmäßig aktiviert. Für Fehleranalysen kann sie deaktiviert werden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.
Polling Anzahl	Legt fest, wie oft bei der Provisionierung oder Synchronisation ins Zielsystem versucht werden soll, einen neu geschriebenen Wert zu lesen, bevor ein Fehler gemeldet wird. Beim Speichern bestimmter Eigenschaften von Benutzerkonten (beispielsweise Telefonnummern oder Instant Messenger Einstellungen) ist das Ergebnis in der G Suite verzögert sichtbar und kann daher erst nach einer Verzögerung für weitere Operationen genutzt werden.
Wiederholversuche bei der Massenverarbeitung	Anzahl der Wiederholversuche für fehlgeschlagene Massenoperationen im Zielsystem, beispielsweise bei der Synchronisation von Gruppenmitgliedschaften.
Timeout bei der Massenverarbeitung	Wartezeit in Sekunden zwischen den Wiederholversuchen für fehlgeschlagene Massenoperationen.
Nutzerdaten vor	Gibt an, ob Nutzerdaten vor dem Löschen von Benutzerkonten, an

Eigenschaft	Beschreibung
dem Löschen transferieren	ein anderes Benutzerkonto übertragen werden sollen. Nutzerdaten, wie beispielsweise Google Drive Daten, Google+ Seiten und Google Kalender, können vor dem endgültigen Löschen des Benutzerkontos an ein anderes Benutzerkonto übertragen werden. Variable: `CP_TransferUserDataBeforeDelete`
Standard-E-Mail-Adresse für Datentransfer	Standard-E-Mail-Adresse des Zielbenutzerkontos für den Transfer von Nutzerdaten, wenn ein Benutzerkonto gelöscht wird. Die E-Mail-Adresse des Zielbenutzerkontos muss eine E-Mail-Adresse aus der primären Domain der Kunden-Umgebung sein, zu der auch das gelöschte Benutzerkonto gehört. Diese E-Mail-Adresse wird genutzt, wenn über den Manager des gelöschten Benutzerkontos keine E-Mail-Adresse ermittelt werden kann. Variable: `CP_DefaultDataTransferTargetEmail`

Produkte und SKUs XML	Produkt-IDs und Stock-Keeping-Unit-IDs als XML-Datei.
	Die Liste der verfügbaren Produkte und SKUs ist durch Google fest definiert und daher auch fest im G Suite Konnektor hinterlegt. Wenn Google diese Liste ändert, kann hier eine XML-Datei eingetragen werden, welche die im G Suite Konnektor hinterlegte Liste überschreibt.
	Beispiel:
	`<products>`
	`<product name="G Suite" id="Google-Apps">`
	`<sku id="Google-Apps-Unlimited" name="G Suite Business"/>`
	`<sku id="Google-Apps-For-Business" name="G Suite Basic" />`
	`<sku id="Google-Apps-Lite" name="G Suite Lite"/>`
	`<sku id="Google-Apps-For-Postini" name="Google Apps Message Security"/>`
	`</product>`
	`<product name="Google Drive storage" id="Google-Drive-storage">`
	`<sku id="Google-Drive-storage-20GB" name="Google Drive storage 20 GB"/>`
	`<sku id="Google-Drive-storage-50GB" name="Google Drive storage 50 GB"/>`

Eigenschaft	Beschreibung

```
            <...>
            <sku id="Google-Drive-storage-16TB" name="Google
            Drive storage 16 TB"/>
        </product>
        <...>
    </products>
```

Verwandte Themen

- Nutzerdaten an ein anderes G Suite Benutzerkonto übertragen auf Seite 134
- API-Bereiche für das Dienstkonto auf Seite 177
- Benutzer und Berechtigungen für die Synchronisation mit einer G Suite auf Seite 15

Verbindungsparameter im Variablenset bearbeiten

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

HINWEIS: Um die Datenkonsistenz in den angebundenen Zielsystemen zu bewahren, stellen Sie sicher, dass die Startkonfiguration für die Synchronisation und das Basisobjekt für die Provisionierung dasselbe Variablenset verwenden. Das gilt insbesondere, wenn ein Synchronisationsprojekt für die Synchronisation verschiedener Kunden-Umgebungen genutzt wird.

Um die erweiterten Einstellungen in einem spezialisierten Variablenset anzupassen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
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 der folgenden Parameter und klicken Sie **Umwandeln**.
   - Polling Anzahl
   - Wiederholversuche bei der Massenverarbeitung

- Timeout bei der Massenverarbeitung
- Lokalen Cache verwenden
- Nur lesender API-Zugriff

Weitere Informationen finden Sie unter Erweiterte Einstellungen der Systemverbindung zur G Suite auf Seite 32.

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*.

Eigenschaften der Zielsystemverbindung bearbeiten

Die erweiterten Einstellungen der Zielsystemverbindung 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 erweiterten Einstellungen mit dem Systemverbindungsassistenten zu bearbeiten

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
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. Auf der Startseite des Systemverbindungsassistenten aktivieren Sie **Erweiterte Einstellungen anzeigen**.
6. Auf der Seite **G Suite Administratoren** können Sie zusätzlich die Option **Nur lesender API-Zugriff** aktivieren.

   Wenn Sie die Verbindung testen, wird geprüft, ob die passenden API-Bereiche autorisiert sind.

   Weitere Informationen finden Sie unter Erweiterte Einstellungen der Systemverbindung zur G Suite auf Seite 32.
7. Auf der Seite **Lokaler Cache** können Sie die Option **Lokalen Cache verwenden** aktivieren.

   Weitere Informationen finden Sie unter Erweiterte Einstellungen der Systemverbindung zur G Suite auf Seite 32.
8. Auf der Seite **Erweiterte Einstellungen** passen Sie die Eigenschaften Ihren Erfordernissen an.

   Weitere Informationen finden Sie unter Erweiterte Einstellungen der Systemverbindung zur G Suite auf Seite 32.
9. Speichern Sie die Änderungen.

Provisionierung von Mitgliedschaften konfigurieren

Mitgliedschaften, beispielsweise von Benutzerkonten in Gruppen, werden in der One Identity Manager-Datenbank in Zuordnungstabellen gespeichert. Bei der Provisionierung von geänderten Mitgliedschaften werden möglicherweise Änderungen, die im Zielsystem

vorgenommen wurden, überschrieben. Dieses Verhalten kann unter folgenden Bedingungen auftreten:

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

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

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

Um die Einzelprovisionierung von Mitgliedschaften zu ermöglichen

1. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **G Suite**.
3. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
4. Wählen Sie die Zuordnungstabellen, für die Sie die Einzelprovisionierung ermöglichen möchten. Mehrfachauswahl ist möglich.
    - Die Option kann nur für Zuordnungstabellen aktiviert werden, deren Basistabelle eine Spalte `XDateSubItem` oder `CCC_XDateSubItem` hat.
    - Zuordnungstabellen, die im Mapping in einer virtuellen Schemaeigenschaft zusammengefasst sind, müssen identisch markiert werden.
5. Klicken Sie **Merge-Modus**.
6. Speichern Sie die Änderungen.

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

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

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

Um die Standardbedingung wiederherzustellen

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

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

Einzelobjektsynchronisation konfigurieren

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

Voraussetzungen

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

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

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

1. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **G Suite**.
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_GAPCustomer).XObjectKey`
8. Speichern Sie die Änderungen.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 44
- Ausstehende Objekte nachbearbeiten auf Seite 45

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.

Die Lastverteilung wird nur für einzelne Provisionierungsprozesse in die G Suite genutzt, um zu verhindern, dass durch die parallele Verarbeitung inkonsistente Daten im Zielsystem entstehen. Keine Lastverteilung erfolgt, wenn die Anzahl der maximalen Instanzen an der Prozessfunktion oder Prozesskomponente auf **1** oder **-1** gesetzt ist.

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

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

Um die Lastverteilung zu konfigurieren

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

   Alle Jobserver müssen auf die gleiche Kunden-Umgebung zugreifen können, wie der Synchronisationsserver für das jeweilige Basisobjekt.
2. Weisen Sie im Synchronization Editor an das Basisobjekt eine kundendefinierte Serverfunktion zu.

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

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

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

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

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

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

Um den Synchronisationsserver ohne Lastverteilung zu nutzen

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

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

Detaillierte Informationen zum Thema

- G Suite Jobserver bearbeiten auf Seite 163

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 42
- Synchronisation deaktivieren auf Seite 44

- Synchronisationsergebnisse anzeigen auf Seite 43

Synchronisationen starten

Beim Einrichten des initialen Synchronisationsprojekts über das Launchpad wird ein Standardzeitplan für regelmäßige Synchronisationen erstellt und zugeordnet. Um regelmäßige Synchronisationen auszuführen, aktivieren Sie diesen Zeitplan.

Um regelmäßige Synchronisationen auszuführen

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

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

Um die initiale Synchronisation manuell zu starten

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

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.

Synchronisationsergebnisse anzeigen

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

Um das Protokoll einer Synchronisation anzuzeigen

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

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

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

Um das Protokoll einer Provisionierung anzuzeigen

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

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

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

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

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

Verwandte Themen

- Synchronisationsprotokoll konfigurieren auf Seite 27
- Fehleranalyse auf Seite 49

Synchronisation deaktivieren

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

Um regelmäßige Synchronisationen zu verhindern

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

   Synchronisationen können nun nur noch manuell gestartet werden.

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

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

Um das Synchronisationsprojekt zu deaktivieren

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

Einzelobjekte synchronisieren

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

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

Um ein Einzelobjekt zu synchronisieren

1. Wählen Sie im Manager die Kategorie **G Suite**.
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.

HINWEIS: Die Aufgabe **Objekt synchronisieren** wird für das in der Ergebnisliste ausgewählte Objekt ausgeführt. Wenn Änderungen an Mitgliedschaften synchronisiert werden sollen, führen Sie die Einzelobjektsynchronisation am Basisobjekt der Zuordnung aus.

Beispiel:

Im Zielsystem wurde einem Nutzer eine Admin-Rolle zugewiesen. Um diese Zuweisung zu synchronisieren, wählen Sie im Manager die Admin-Rollen-Zuordnung, der das Benutzerkonto zugewiesen wurde, und führen Sie die Einzelobjektsynchronisation aus. Dabei werden alle Mitgliedschaften für diese Admin-Rollen-Zuordnung synchronisiert. Wenn die Einzelobjektsynchronisation am Benutzerkonto ausgeführt wird, werden keine Mitgliedschaften synchronisiert, da die Tabelle `GAPUser` nicht die Basistabelle der Zuordnung darstellt.

Die Basistabelle einer Zuordnung enthält eine Spalte `XDateSubItem` mit der Information über die letzte Änderung der Mitgliedschaften.

Detaillierte Informationen zum Thema

- Einzelobjektsynchronisation konfigurieren auf Seite 39

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 nachbearbeiten auf Seite 45
- Benutzerkonten über Kontendefinitionen verwalten auf Seite 48

Ausstehende Objekte nachbearbeiten

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 **G Suite | Zielsystemabgleich: G Suite**.

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

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

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

   - Das Synchronisationsprotokoll wurde bereits gelöscht.

     - ODER -

   - Im Zielsystem wurde eine Zuweisung aus einer Mitgliederliste gelöscht.

     Bei der Synchronisation wird das Basisobjekt der Zuordnung aktualisiert. Dafür erscheint ein Eintrag im Synchronisationsprotokoll. Der Eintrag in der Zuordnungstabelle wird als ausstehend markiert, es gibt jedoch keinen Eintrag im Synchronisationsprotokoll.

   - Im Zielsystem wurde ein Objekt gelöscht, das eine Mitgliederliste enthält.

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

   TIPP:

   Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

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

   b. Öffnen Sie das Kontextmenü und klicken Sie **Objekt anzeigen**.

3. Wählen Sie die Objekte, die Sie nachbearbeiten möchten. Mehrfachauswahl ist möglich.

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

Tabelle 10: Methoden zur Behandlung ausstehender Objekte

Symbol	Methode	Beschreibung
	Löschen	Das Objekt wird sofort in der One Identity Manager-Datenbank gelöscht. Eine Löschverzögerung wird nicht berücksichtigt. Die Markierung **Ausstehend** wird für das Objekt entfernt. Indirekte Mitgliedschaften können nicht gelöscht werden.

Symbol	Methode	Beschreibung
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung **Ausstehend** wird für das Objekt entfernt. Die Methode löst das Ereignis `HandleOutstanding` aus. Dadurch wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt. Voraussetzungen: • Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen. • Der Zielsystemkonnektor kann schreibend auf das Zielsystem zugreifen.
	Zurücksetzen	Die Markierung **Ausstehend** wird für das Objekt entfernt.

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

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

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

Um die Massenverarbeitung zu deaktivieren

- Deaktivieren Sie in der Formularsymbolleiste  .

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

Verwandte Themen

- Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen auf Seite 48
- Erweiterte Einstellungen der Systemverbindung zur G Suite auf Seite 32

Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen

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

Um Tabellen in den Zielsystemabgleich aufzunehmen

1. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **G Suite**.
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 nachbearbeiten auf Seite 45

Benutzerkonten über Kontendefinitionen verwalten

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

Um die Benutzerkonten über Kontendefinitionen zu verwalten, weisen Sie diesen Benutzerkonten eine Kontendefinition und einen Automatisierungsgrad zu.

Detaillierte Informationen zum Thema

- Kontendefinitionen an verbundene Benutzerkonten zuweisen auf Seite 74

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 43

3

Managen von G Suite Benutzerkonten und Personen

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

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

- Personen erhalten ihre Benutzerkonten automatisch über Kontendefinitionen. Hat eine Person noch kein Benutzerkonto in einer Kunden-Umgebung, wird durch die Zuweisung der Kontendefinition an eine Person über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

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

- Personen und Benutzerkonten können manuell erfasst und einander zugeordnet werden.

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

Verwandte Themen

- Kontendefinitionen für G Suite Benutzerkonten auf Seite 51
- Automatische Zuordnung von Personen zu G Suite Benutzerkonten auf Seite 69
- Stammdaten für G Suite Benutzerkonten bearbeiten auf Seite 119

Kontendefinitionen für G Suite Benutzerkonten

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

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

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

Ausführliche Informationen zu den Grundlagen zu Kontendefinitionen, Automatisierungsgraden und zur Ermittlung der gültigen IT Betriebsdaten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

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

Detaillierte Informationen zum Thema

- Kontendefinitionen erstellen auf Seite 52
- Automatisierungsgrade bearbeiten auf Seite 55
- Abbildungsvorschriften für IT Betriebsdaten erstellen auf Seite 57
- IT Betriebsdaten erfassen auf Seite 59
- Zuweisen der Kontendefinitionen an Personen auf Seite 61
- Kontendefinitionen an Zielsysteme zuweisen auf Seite 66

Kontendefinitionen erstellen

Um eine Kontendefinition zu erstellen

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

Verwandte Themen

- Stammdaten von Kontendefinitionen auf Seite 53
- Kontendefinitionen bearbeiten auf Seite 52

Kontendefinitionen bearbeiten

Um eine Kontendefinition zu bearbeiten

1. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten der Kontendefinition.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von Kontendefinitionen auf Seite 53
- Kontendefinitionen erstellen auf Seite 52

Stammdaten von Kontendefinitionen

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 11: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte Kontendefinition	Vorausgesetzte Kontendefinition. Definieren Sie Abhängigkeiten zwischen. Wenn die bestellt oder zugeordnet wird, wird die vorausgesetzte automatisch mitbestellt oder zugeordnet. Für eine G Suite lassen Sie die Angabe leer.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatisierungsgrad (initial)	Standardautomatisierungsgrad, der bei Neuanlage von Benutzerkonten standardmäßig verwendet werden soll.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Kontendefinition an Personen. Erfassen Sie einen Wert zwischen 0 und 1. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Leistungsposition	Leistungsposition, über welche die Kontendefinition im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.
IT Shop	Angabe, ob die Kontendefinition über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Personen und Rollen außerhalb des IT Shop zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von den Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig.

Eigenschaft	Beschreibung
Automatische Zuweisung zu Personen	Angabe, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Beim Speichern wird die Kontendefinition an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine Person neu angelegt wird, erhält sie ebenfalls automatisch diese Kontendefinition. WICHTIG: Aktivieren Sie diese Option nur, wenn sichergestellt ist, dass alle aktuell in der Datenbank vorhandenen internen Personen sowie alle zukünftig neu hinzuzufügenden internen Personen ein Benutzerkonto in diesem Zielsystem erhalten sollen! Um die automatische Zuweisung der Kontendefinition an alle Personen zu entfernen, deaktivieren Sie die Option. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.
Kontendefinition bei dauerhafter Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei zeitweiliger Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei verzögertem Löschen beibehalten	Angabe zur Zuweisung der Kontendefinition bei verzögertem Löschen von Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei Sicherheitsgefährdung beibehalten	Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.

Eigenschaft	Beschreibung
Ressourcentyp	Ressourcentyp zur Gruppierung von Kontendefinitionen.
Freies Feld 01- Freies Feld 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Automatisierungsgrade bearbeiten

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

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

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kontendefinitionen | Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Automatisierungsgrades.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von Automatisierungsgraden auf Seite 56
- Automatisierungsgrade erstellen auf Seite 56

Automatisierungsgrade erstellen

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

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

Um einen Automatisierungsgrad zu erstellen

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

Verwandte Themen

- Stammdaten von Automatisierungsgraden auf Seite 56
- Automatisierungsgrade bearbeiten auf Seite 55

Stammdaten von Automatisierungsgraden

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 12: Stammdaten eines Automatisierungsgrades

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

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

Abbildungsvorschriften für IT Betriebsdaten erstellen

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

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

- G Suite Organisation
- Gruppen erbbar

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

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

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

Tabelle 13: Abbildungsvorschrift für IT Betriebsdaten

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

Eigenschaft	Beschreibung
	Benutzerkontos mit Standardwerten verwendet. Um die Mailvorlage zu ändern, passen Sie den Konfigurationsparameter **TargetSystem | GoogleApps | Accounts | MailTemplateDefaultValues** an.

4. Speichern Sie die Änderungen.

IT Betriebsdaten erfassen

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

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

Beispiel

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

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

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

Um IT Betriebsdaten festzulegen

1. Wählen Sie im Manager in der Kategorie **Organisationen** oder **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten**.
3. Klicken Sie **Hinzufügen** und erfassen Sie die folgenden Daten.

Tabelle 14: IT Betriebsdaten

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

4. Speichern Sie die Änderungen.

Verwandte Themen

- Abbildungsvorschriften für IT Betriebsdaten erstellen auf Seite 57

IT Betriebsdaten ändern

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

Voraussetzungen

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

  - ODER -

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

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

Um die Bildungsregeln auszuführen

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

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

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

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

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinitionen an Personen

Kontendefinitionen werden an die Personen des Unternehmens zugewiesen.

Das Standardverfahren für die Zuweisung von Kontendefinitionen an Personen ist die indirekte Zuweisung. Die Kontendefinitionen werden an die Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen zugewiesen. Die Personen werden gemäß ihrer Funktion im Unternehmen in diese Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen

eingeordnet und erhalten so ihre Kontendefinitionen. Um auf Sonderanforderungen zu reagieren, können einzelne Kontendefinitionen direkt an Personen zugewiesen werden.

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

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

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

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

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

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

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

Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
    - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
    - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
    - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Organisation und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Kontendefinitionen an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

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

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Kontendefinitionen an alle Personen zuweisen

Um eine Kontendefinition an alle Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.

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

5. Speichern Sie die Änderungen.

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

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

Kontendefinitionen direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

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

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

   Um eine Zuweisung zu entfernen

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

Kontendefinitionen an Systemrollen zuweisen

Installierte Module: Systemrollenmodul

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

Um Kontendefinitionen in eine Systemrolle aufzunehmen

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

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Systemrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Kontendefinitionen in den IT Shop aufnehmen

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

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

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

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

Um eine Kontendefinition in den IT Shop aufzunehmen

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

   - ODER -

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

Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen

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

   - ODER -

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

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

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

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

   - ODER -

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

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

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

Verwandte Themen

- Stammdaten von Kontendefinitionen auf Seite 53

Kontendefinitionen an Zielsysteme zuweisen

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

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

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

Um die Kontendefinition an ein Zielsystem zuzuweisen

1. Wählen Sie im Manager in der Kategorie **G Suite | Kunden-Umgebungen** die Kunden-Umgebung.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie in der Auswahlliste **Kontendefinition (initial)** die Kontendefinition für die Benutzerkonten.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Automatische Zuordnung von Personen zu G Suite Benutzerkonten auf Seite 69

Kontendefinitionen löschen

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

Um eine Kontendefinition zu löschen

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

c. Wählen Sie die Aufgabe **Organisationen zuweisen**.

d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Abteilungen, Kostenstellen und Standorte.

e. Speichern Sie die Änderungen.

4. Entfernen Sie die Zuordnung der Kontendefinition zu Geschäftsrollen.

   a. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

   c. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.

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

   d. Speichern Sie die Änderungen.

5. Wenn die Kontendefinition über den IT Shop bestellt wurde, muss sie abbestellt und aus allen IT Shop Regalen entfernt werden.

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

   Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

   a. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

      - ODER -

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

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

   c. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.

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

   e. Klicken Sie **OK**.

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

6. Entfernen Sie die Zuordnung der Kontendefinition als vorausgesetzte Kontendefinition einer anderen Kontendefinition. Solange die Kontendefinition Voraussetzung einer anderen Kontendefinition ist, kann sie nicht gelöscht werden. Prüfen Sie alle Kontendefinitionen.

   a. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

   c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   d. Entfernen Sie in der Auswahlliste **Vorausgesetzte Kontendefinition** die

Kontendefinition.

e. Speichern Sie die Änderungen.

7. Entfernen Sie die Zuordnung der Kontendefinition zum Zielsystem.
   a. Wählen Sie im Manager in der Kategorie **G Suite | Kunden-Umgebungen** die Kunden-Umgebung.
   b. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
   c. Entfernen Sie auf dem Tabreiter **Allgemein** die zugewiesenen Kontendefinitionen.
   d. Speichern Sie die Änderungen.
8. Löschen Sie die Kontendefinition.
   a. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
   b. Wählen Sie in der Ergebnisliste die Kontendefinition.
   c. Klicken Sie , um die Kontendefinition zu löschen.

Automatische Zuordnung von Personen zu G Suite Benutzerkonten

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

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

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

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

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

  Beispiel:

  ```
  ADMINISTRATOR*
  ```

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

HINWEIS:

Für die Synchronisation gilt:

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

Außerhalb der Synchronisation gilt:

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

HINWEIS:

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

Um die Benutzerkonten über Kontendefinitionen zu verwalten, weisen Sie diesen Benutzerkonten eine Kontendefinition und einen Automatisierungsgrad zu.

Weitere Informationen finden Sie unter Benutzerkonten über Kontendefinitionen verwalten auf Seite 48.

Ausführliche Informationen zur automatischen Personenzuordnung finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Kontendefinitionen erstellen auf Seite 52
- Kontendefinitionen an Zielsysteme zuweisen auf Seite 66
- Automatisierungsgrad an G Suite Benutzerkonten ändern auf Seite 74
- Suchkriterien für die automatische Personenzuordnung bearbeiten auf Seite 71

Suchkriterien für die automatische Personenzuordnung bearbeiten

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

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

HINWEIS: Bei der Zuordnung der Personen zu Benutzerkonten anhand der Suchkriterien erhalten die Benutzerkonten den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Abhängig davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden.

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

Um Kriterien für die Personenzuordnung festzulegen

1. Wählen Sie im Manager die Kategorie **G Suite | G Suite Kunden**.
2. Wählen Sie in der Ergebnisliste die Kunden-Umgebung.
3. Wählen Sie die Aufgabe **Suchkriterien für die Personenzuordnung definieren**.
4. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person mit dem

Benutzerkonto verbunden wird.

Tabelle 15: Standardsuchkriterien für Benutzerkonten

Anwenden auf	Spalte an Person	Spalte am Benutzerkonto
G Suite Benutzerkonten	Standard-E-Mail-Adresse (`DefaultEmailAddress`)	Primäre E-Mail-Adresse (`PrimaryEmail`)

5. Speichern Sie die Änderungen.

Ausführliche Informationen zur Definition der Suchkriterien finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Automatische Zuordnung von Personen zu G Suite Benutzerkonten auf Seite 69
- Personen suchen und direkt an Benutzerkonten zuordnen auf Seite 72

Personen suchen und direkt an Benutzerkonten zuordnen

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

Tabelle 16: Ansichten zur manuellen Zuordnung

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

Um Suchkriterien auf die Benutzerkonten anzuwenden

1. Wählen Sie im Manager die Kategorie **G Suite | G Suite Kunden**.
2. Wählen Sie in der Ergebnisliste die Kunden-Umgebung.

3. Wählen Sie die Aufgabe **Suchkriterien für die Personenzuordnung definieren**.
4. Im unteren Bereich des Formulars klicken Sie **Neu laden**.

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

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

Durch die Zuordnung von Personen an die Benutzerkonten entstehen verbundene Benutzerkonten (Zustand **Linked**). Um verwaltete Benutzerkonten zu erhalten (Zustand **Linked configured**), können Sie gleichzeitig eine Kontendefinition zuordnen.

Um Personen direkt über die Vorschlagsliste zuzuordnen

- Klicken Sie **Vorgeschlagene Zuordnungen**.
  1. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die vorgeschlagene Person zugeordnet werden soll. Eine Mehrfachauswahl ist möglich.
  2. (Optional) Wählen Sie im Auswahlfeld **Diese Kontendefinition zuweisen** eine Kontendefinition und im Auswahlfeld **Diesen Automatisierungsgrad zuweisen** einen Automatisierungsgrad.
  3. Klicken Sie **Ausgewählte zuweisen.**
  4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

     Den ausgewählten Benutzerkonten werden die per Suchkriterium ermittelten Personen zugeordnet. Wenn eine Kontendefinition ausgewählt wurde, wird diese an alle ausgewählten Benutzerkonten zugeordnet.

  - ODER -

- Klicken Sie **Ohne Personenzuordnung**.
  1. Klicken Sie **Person auswählen** für das Benutzerkonto, dem eine Person zugeordnet werden soll. Wählen Sie eine Person aus der Auswahlliste.
  2. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die ausgewählten Personen zugeordnet werden sollen. Eine Mehrfachauswahl ist möglich.
  3. (Optional) Wählen Sie im Auswahlfeld **Diese Kontendefinition zuweisen** eine Kontendefinition und im Auswahlfeld **Diesen Automatisierungsgrad zuweisen** einen Automatisierungsgrad.
  4. Klicken Sie **Ausgewählte zuweisen**.
  5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

     Den ausgewählten Benutzerkonten werden die Personen zugeordnet, die in der Spalte **Person** angezeigt werden. Wenn eine Kontendefinition ausgewählt wurde, wird diese an alle ausgewählten Benutzerkonten zugeordnet.

Um Zuordnungen zu entfernen

- Klicken Sie **Zugeordnete Benutzerkonten**.
    1. Klicken Sie **Auswahl** für alle Benutzerkonten, deren Personenzuordnung entfernt werden soll. Mehrfachauswahl ist möglich.
    2. Klicken Sie **Ausgewählte entfernen**.
    3. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

       Von den ausgewählten Benutzerkonten werden die zugeordneten Personen entfernt.

Automatisierungsgrad an G Suite Benutzerkonten ändern

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

Um den Automatisierungsgrad für ein Benutzerkonto zu ändern

1. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Automatisierungsgrad** den Automatisierungsgrad.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für G Suite Benutzerkonten auf Seite 120

Kontendefinitionen an verbundene Benutzerkonten zuweisen

An Benutzerkonten im Zustand **Linked** (verbunden) kann nachträglich eine Kontendefinition zugewiesen werden. Das kann beispielsweise erforderlich sein, wenn

- Personen und Benutzerkonten manuell verbunden wurden
- die automatische Personzuordnung konfiguriert ist, beim Einfügen eines Benutzerkontos jedoch noch keine Kontendefinition an die Kunden-Umgebung zugeordnet ist

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie der Kunden-Umgebung die Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand **Linked** (verbunden) die Kontendefinition zu. Es wird der Standardautomatisierungsgrad der Kontendefinition für das Benutzerkonto übernommen.
    a. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten | Verbunden aber nicht konfiguriert | <Kunden-Umgebung>**.
    b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.
    c. Wählen Sie in der Auswahlliste **Kontendefinition** die Kontendefinition.
    d. Wählen Sie die Benutzerkonten, die die Kontendefinition erhalten sollen.
    e. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Kontendefinitionen für G Suite Benutzerkonten auf Seite 51
- Kontendefinitionen an Zielsysteme zuweisen auf Seite 66

Personen manuell mit G Suite Benutzerkonten verbinden

Eine Person kann mit mehreren G Suite Benutzerkonten verbunden werden, beispielsweise um zusätzlich zum Standardbenutzerkonto ein administratives Benutzerkonto zuzuweisen. Darüber hinaus kann eine Person Standardbenutzerkonten mit verschiedenen Typen nutzen.

HINWEIS: Um mit Identitäten für Benutzerkonten zu arbeiten, benötigen die Personen ebenfalls Identitäten. Benutzerkonten, denen eine Identität zugeordnet ist, können Sie nur mit Personen verbinden, die dieselbe Identität haben.

Um einer Person manuell Benutzerkonten zuzuweisen

1. Wählen Sie im Manager die Kategorie **Personen | Personen**.
2. Wählen Sie in der Ergebnisliste die Person und führen Sie die Aufgabe **G Suite Benutzerkonten zuweisen** aus.
3. Weisen Sie die Benutzerkonten zu.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Unterstützte Typen von Benutzerkonten auf Seite 76

Unterstützte Typen von Benutzerkonten

Im One Identity Manager können unterschiedliche Typen von Benutzerkonten wie beispielsweise Standardbenutzerkonten, administrative Benutzerkonten, Dienstkonten oder privilegierte Benutzerkonten abgebildet werden.

Zur Abbildung der verschiedenen Benutzerkontentypen werden die folgenden Eigenschaften verwendet.

- Identität

  Mit der Eigenschaft **Identität** (Spalte `IdentityType`) wird der Typ des Benutzerkontos beschrieben.

  Tabelle 17: Identitäten von Benutzerkonten

Identität	Beschreibung	Wert der Spalte IdentityType
Primäre Identität	Standardbenutzerkonto einer Person.	Primary
Organisatorische Identität	Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen.	Organizational
Persönliche Administratoridentität	Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird.	Admin
Zusatzidentität	Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird.	Sponsored
Gruppenidentität	Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird.	Shared
Dienstidentität	Dienstkonto.	Service

  HINWEIS: Um mit Identitäten für Benutzerkonten zu arbeiten, benötigen die Personen ebenfalls Identitäten. Benutzerkonten, denen eine Identität zugeordnet ist, können Sie nur mit Personen verbinden, die dieselbe Identität haben.

  Die primäre Identität, die organisatorische Identität und die persönliche Administratoridentität werden für die verschiedenen Benutzerkonten genutzt, mit denen ein und dieselbe Person ihre unterschiedlichen Aufgaben im Unternehmen ausführen kann.

  Um Benutzerkonten mit einer persönlichen Administratoridentität oder einer organisatorische Identität für eine Person bereitzustellen, richten Sie für die Person

Subidentitäten ein. Diese Subidentitäten verbinden Sie mit den Benutzerkonten. Somit können für die unterschiedlichen Benutzerkonten die erforderlichen Berechtigungen erteilt werden.

Benutzerkonten mit einer Zusatzidentität, einer Gruppenidentität oder einer Dienstidentität verbinden Sie mit Dummy-Personen, die keinen Bezug zu einer realen Person haben. Diese Dummy-Personen werden benötigt, um Berechtigungen an die Benutzerkonten vererben zu können. Bei der Auswertung von Berichten, Attestierungen oder Complianceprüfungen prüfen Sie, ob die Dummy-Personen gesondert betrachtet werden müssen.

Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

- Privilegiertes Benutzerkonto

  Privilegierte Benutzerkonten werden eingesetzt, um Personen mit zusätzlichen privilegierten Berechtigungen auszustatten. Dazu gehören beispielsweise administrative Benutzerkonten oder Dienstkonten. Die Benutzerkonten werden mit der Eigenschaft **Privilegiertes Benutzerkonto** (Spalte `IsPrivilegedAccount`) gekennzeichnet.

Detaillierte Informationen zum Thema

- Standardbenutzerkonten auf Seite 77
- Administrative Benutzerkonten auf Seite 78
- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 79
- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 80
- Privilegierte Benutzerkonten auf Seite 81

Standardbenutzerkonten

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

Um Standardbenutzerkonten über Kontendefinitionen zu erstellen

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

3. Erstellen Sie eine Abbildungsvorschrift für die IT Betriebsdaten.

   Mit der Abbildungsvorschrift legen Sie fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über primären Rollen einer Person ermittelt werden können.

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

   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IsGroupAccount` den Standardwert **1** und aktivieren Sie die Option **Immer Standardwert verwenden**.
   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IdentityType` den Standardwert **Primary** und aktivieren Sie die Option **Immer Standardwert verwenden**.
4. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem. Wählen Sie unter **Wirksam für** das konkrete Zielsystem.

   Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.
5. Weisen Sie die Kontendefinition an die Personen zu.

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

Verwandte Themen

- Kontendefinitionen für G Suite Benutzerkonten auf Seite 51

Administrative Benutzerkonten

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

Administrative Benutzerkonten werden durch die Synchronisation in den One Identity Manager eingelesen.

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

Verwandte Themen

- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 79
- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 80

Administrative Benutzerkonten für eine Person bereitstellen

Voraussetzungen

- Das Benutzerkonto muss als persönliche Administratoridentität gekennzeichnet sein.
- Die Person, die das Benutzerkonto nutzen soll, muss als persönliche Administratoridentität gekennzeichnet sein.
- Die Person, die das Benutzerkonto nutzen soll, muss mit einer Hauptidentität verbunden sein.

Um ein administratives Benutzerkonto für eine Person bereitzustellen

1. Kennzeichnen Sie das Benutzerkonto als persönliche Administratoridentität.
    a. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Identität** den Wert **Persönliche Administratoridentität**.
2. Verbinden Sie das Benutzerkonto mit der Person, die dieses administrative Benutzerkonto nutzen soll.
    a. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Person** die Person, die dieses administrative Benutzerkonto nutzt.

    TIPP: Als Zielsystemverantwortlicher können Sie über die Schaltfläche eine neue Person erstellen.

Verwandte Themen

- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 80
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Administrative Benutzerkonten für mehrere Personen bereitstellen

Voraussetzung

- Das Benutzerkonto muss als Gruppenidentität gekennzeichnet sein.
- Es muss eine Dummy-Person vorhanden sein. Die Dummy-Person muss als Gruppenidentität gekennzeichnet sein und muss einen Manager besitzen.
- Die Personen, die das Benutzerkonto nutzen dürfen, müssen als primäre Identitäten gekennzeichnet sein.

Um ein administratives Benutzerkonto für mehrere Personen bereitzustellen

1. Kennzeichnen Sie das Benutzerkonto als Gruppenidentität.
    a. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Identität** den Wert **Gruppenidentität**.
2. Verbinden Sie das Benutzerkonto mit einer Dummy-Person.
    a. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Person** die Dummy-Person.

    TIPP: Als Zielsystemverantwortlicher können Sie über die Schaltfläche eine neue Dummy-Person erstellen.
3. Weisen Sie dem Benutzerkonto die Personen zu, die dieses administrative Benutzerkonto nutzen sollen.
    a. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Personen mit Nutzungsberechtigungen zuzuweisen**.
    d. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

    Um eine Zuweisung zu entfernen

    - Wählen Sie die Person und doppelklicken Sie .

Verwandte Themen

- Administrative Benutzerkonten für eine Person bereitstellen
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Privilegierte Benutzerkonten

Privilegierte Benutzerkonten werden eingesetzt, um Personen mit zusätzlichen privilegierten Berechtigungen auszustatten. Dazu gehören beispielsweise administrative Benutzerkonten oder Dienstkonten. Die Benutzerkonten werden mit der Eigenschaft **Privilegiertes Benutzerkonto** (Spalte `IsPrivilegedAccount`) gekennzeichnet.

HINWEIS: Die Kriterien anhand derer Benutzerkonten automatisch als privilegiert erkannt werden, sind als Erweiterungen zur Sichtdefinition (ViewAddOn) an der Tabelle `TSBVAccountIsPrivDetectRule` (Tabelle vom Typ **Union**) definiert. Die Auswertung erfolgt im Skript `TSB_SetIsPrivilegedAccount`.

Um privilegierte Benutzerkonten über Kontendefinitionen zu erstellen

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

   Mit der Abbildungsvorschrift legen Sie fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden, und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über primären Rollen einer Person ermittelt werden können.

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

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

- Zusätzlich können Sie eine Abbildungsvorschrift für die Spalte `IdentityType` festlegen. Die Spalte besitzt verschiedene zulässige Werte, die privilegierte Benutzerkonten repräsentieren.
- Um zu verhindern, das privilegierte Benutzerkonten die Berechtigungen des Standardbenutzers erben, definieren Sie eine Abbildungsvorschrift für die Spalte `IsGroupAccount` mit dem Standardwert **0** und aktivieren Sie die Option **Immer Standardwert verwenden**.

5. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem.

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

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

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

TIPP: Wenn es unternehmensspezifisch erforderlich ist, dass die primären E-Mail-Adressen privilegierter Benutzerkonten einem definierten Namensschema folgen, legen Sie die Bildungsregel fest, nach der die primären E-Mail-Adressen gebildet werden.

Verwandte Themen

- Kontendefinitionen für G Suite Benutzerkonten auf Seite 51

4

Bereitstellen von Anmeldeinformationen für G Suite Benutzerkonten

Wenn neue Benutzerkonten im One Identity Manager angelegt werden, werden sofort auch die zur Anmeldung am Zielsystem benötigten Kennwörter erstellt. Um das initiale Kennwort zu vergeben, stehen verschiedene Möglichkeiten zur Verfügung. Auf die Kennwörter werden vordefinierte Kennwortrichtlinien angewendet, die Sie bei Bedarf an Ihre Anforderungen anpassen können. Um die generierten Anmeldeinformationen an die Benutzer zu verteilen, können Sie E-Mail-Benachrichtigungen einrichten.

Detaillierte Informationen zum Thema

- Kennwortrichtlinien für G Suite Benutzerkonten auf Seite 83
- Initiales Kennwort für neue G Suite Benutzerkonten auf Seite 95
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 95

Kennwortrichtlinien für G Suite Benutzerkonten

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

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

Detaillierte Informationen zum Thema

- Vordefinierte Kennwortrichtlinien auf Seite 84
- Kennwortrichtlinien anwenden auf Seite 85
- Kennwortrichtlinien erstellen auf Seite 87
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 91
- Ausschlussliste für Kennwörter bearbeiten auf Seite 93
- Kennwörter prüfen auf Seite 94
- Generieren von Kennwörtern testen auf Seite 94

Vordefinierte Kennwortrichtlinien

Die vordefinierte Kennwortrichtlinien können Sie bei Bedarf an Ihre Anforderungen anpassen.

Kennwortrichtlinie für die Anmeldung am One Identity Manager

Für die Anmeldung am One Identity Manager wird die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** angewendet. Diese Kennwortrichtlinie definiert die Einstellung für die Kennwörter von Systembenutzern (`DialogUser.Password` und `Person.DialogUserPassword`) sowie für den Zugangscode für die einmalige Anmeldung am Web Portal (`Person.Passcode`).

HINWEIS: Die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn keine andere Kennwortrichtlinie für Personen, Benutzerkonten oder Systembenutzer ermittelt werden kann.

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

Kennwortrichtlinie für die Bildung des zentralen Kennwortes von Personen

Bei entsprechender Konfiguration wird das zentrale Kennwort einer Person auf die Kennwörter der zielsystemspezifischen Benutzerkonten abgebildet. Die Kennwortrichtlinie **Kennwortrichtlinie für zentrales Kennwort von Personen** definiert die Einstellung für das zentrale Kennwort (`Person.CentralPassword`). Die Mitglieder der Anwendungsrolle **Identity Management | Personen | Administratoren** können diese Kennwortrichtlinie anpassen.

WICHTIG: Stellen Sie sicher, dass die Kennwortrichtlinie **Kennwortrichtlinie für zentrales Kennwort von Personen** nicht gegen die zielsystemspezifischen Anforderungen an Kennwörter verstößt.

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

Kennwortrichtlinien für Benutzerkonten

Es werden vordefinierte Kennwortrichtlinien bereitgestellt, die Sie auf die Kennwortspalten der Benutzerkonten anwenden können.

WICHTIG: Wenn Sie nicht mit zielsystemspezifischen Kennwortrichtlinien arbeiten, wirkt die Standardrichtlinie **One Identity Manager Kennwortrichtlinie**. Stellen Sie in diesem Fall sicher, dass die Standardrichtlinie nicht gegen die Anforderungen der Zielsysteme verstößt.

Für Kunden-Umgebungen ist die Kennwortrichtlinie **G Suite Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Benutzerkonten (`GAPUser.Password`) einer Kunden-Umgebung anwenden.

Wenn die Kennwortanforderungen der Kunden-Umgebungen unterschiedlich sind, wird empfohlen, je Kunden-Umgebung eine eigene Kennwortrichtlinie einzurichten.

Des Weiteren können Sie Kennwortrichtlinien abhängig von der Kontendefinition der Benutzerkonten oder abhängig vom Automatisierungsgrad der Benutzerkonten anwenden.

Kennwortrichtlinien anwenden

Für Kunden-Umgebungen ist die Kennwortrichtlinie **G Suite Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Benutzerkonten (`GAPUser.Password`) einer Kunden-Umgebung anwenden.

Wenn die Kennwortanforderungen der Kunden-Umgebungen unterschiedlich sind, wird empfohlen, je Kunden-Umgebung eine eigene Kennwortrichtlinie einzurichten.

Des Weiteren können Sie Kennwortrichtlinien abhängig von der Kontendefinition der Benutzerkonten oder abhängig vom Automatisierungsgrad der Benutzerkonten anwenden.

Die anzuwendende Kennwortrichtlinie für ein Benutzerkonto wird in folgender Reihenfolge ermittelt:

1. Kennwortrichtlinie der Kontendefinition des Benutzerkontos
2. Kennwortrichtlinie des Automatisierungsgrades des Benutzerkontos
3. Kennwortrichtlinie der G Suite Kunden-Umgebung des Benutzerkontos
4. Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** (Standardrichtlinie)

WICHTIG: Wenn Sie nicht mit zielsystemspezifischen Kennwortrichtlinien arbeiten, wirkt die Standardrichtlinie **One Identity Manager Kennwortrichtlinie**. Stellen Sie in diesem Fall sicher, dass die Standardrichtlinie nicht gegen die Anforderungen der Zielsysteme verstößt.

Um eine Kennwortrichtlinie neu zuzuweisen

1. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.

3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Klicken Sie im Bereich **Zuweisungen** die Schaltfläche **Hinzufügen** und erfassen Sie folgende Daten.

Tabelle 18: Zuweisen einer Kennwortrichtlinie

Eigenschaft	Beschreibung
Anwenden auf	Anwendungsbereich der Kennwortrichtlinie. ***Um den Anwendungsbereich festzulegen*** a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. b. Wählen Sie unter **Tabelle** eine der folgenden Referenzen: • Die Tabelle, die die Basisobjekte der Synchronisation enthält. • Um die Kennwortrichtlinie abhängig von der Kontendefinition anzuwenden, wählen Sie die Tabelle `TSBAccountDef`. • Um die Kennwortrichtlinie abhängig vom Automatisierungsgrad anzuwenden, wählen Sie die Tabelle `TSBBehavoir`. c. Wählen Sie unter **Anwenden auf** die Tabelle, die die Basisobjekte enthält. • Wenn Sie die Tabelle mit den Basisobjekten der Synchronisation gewählt haben, dann wählen Sie das konkrete Zielsystem. • Wenn Sie die Tabelle `TSBAccountDef` gewählt haben, dann wählen Sie die konkrete Kontendefinition. • Wenn Sie die Tabelle `TSBBehavior` gewählt haben, dann wählen Sie den konkreten Automatisierungsgrad. d. Klicken Sie **OK**.
Kennwortspalte	Bezeichnung der Kennwortspalte.
Kennwortrichtlinie	Bezeichnung der Kennwortrichtlinie, die angewendet werden soll.

5. Speichern Sie die Änderungen.

Um die Zuweisung einer Kennwortrichtlinie zu ändern

1. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.

3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Wählen Sie im Bereich **Zuweisungen** die Zuweisung, die Sie ändern möchten.
5. Wählen Sie in der Auswahlliste **Kennwortrichtlinie** die neu anzuwendende Kennwortrichtlinie.
6. Speichern Sie die Änderungen.

Kennwortrichtlinien bearbeiten

Um eine Kennwortrichtlinie zu bearbeiten

1. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten der Kennwortrichtlinie.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Kennwortrichtlinie auf Seite 88
- Richtlinieneinstellungen auf Seite 88
- Zeichenklassen für Kennwörter auf Seite 90
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 91

Kennwortrichtlinien erstellen

Um eine Kennwortrichtlinie zu erstellen

1. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular erfassen Sie die Stammdaten der Kennwortrichtlinie.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Kennwortrichtlinie auf Seite 88
- Richtlinieneinstellungen auf Seite 88

- Zeichenklassen für Kennwörter auf Seite 90
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 91

Allgemeine Stammdaten einer Kennwortrichtlinie

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 19: Stammdaten einer Kennwortrichtlinie

Eigenschaft	Bedeutung
Anzeigename	Bezeichnung der Kennwortrichtlinie. Übersetzen Sie den eingegebenen Text über die Schaltfläche.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.Übersetzen Sie den eingegebenen Text über die Schaltfläche.
Fehlermeldung	Kundenspezifische Fehlermeldung, die ausgegeben wird, wenn die Richtlinie nicht erfüllt wird. Übersetzen Sie den eingegebenen Text über die Schaltfläche.
Eigentümer (Anwendungsrolle)	Anwendungsrolle, deren Mitglieder die Kennwortrichtlinie konfigurieren können.
Standardrichtlinie	Kennzeichnung als Standardrichtlinie für Kennwörter. HINWEIS: Die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn keine andere Kennwortrichtlinie für Personen, Benutzerkonten oder Systembenutzer ermittelt werden kann.

Richtlinieneinstellungen

Auf dem Tabreiter **Kennwort** definieren Sie folgende Einstellungen für eine Kennwortrichtlinie.

Tabelle 20: Richtlinieneinstellungen

Eigenschaft	Bedeutung
Initiales Kennwort	Initiales Kennwort für neu erzeugte Benutzerkonten. Wird beim Erstellen eines Benutzerkontos kein Kennwort angegeben oder kein Zufallskennwort generiert, dann wird das initiale Kennwort benutzt.

Eigenschaft	Bedeutung
Kennwortbestätigung	Kennwortwiederholung.
Min. Länge	Minimale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben muss.
Max. Länge	Maximale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben kann. Der maximal zulässige Wert ist **256**.
Max. Fehlanmeldungen	Anzahl der maximalen Fehlanmeldungen. Legen Sie die Anzahl der ungültigen Kennworteingaben fest. Wird nur berücksichtigt, bei Anmeldung am One Identity Manager. Die Angabe wird nur berücksichtigt, wenn die Anmeldung am One Identity Manager mit einem Systembenutzer- oder Personen-basierten Authentifizierungsmodul erfolgt. Hat ein Benutzer die Anzahl der maximalen Fehlanmeldungen erreicht, kann sich die Person oder der Systembenutzer nicht mehr am One Identity Manager anmelden. Kennwörter gesperrter Personen und Systembenutzer können im Kennwortrücksetzungsportal zurückgesetzt werden. Ausführliche Informationen finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.
Max. Tage gültig	Maximales Alter des Kennwortes. Geben Sie die Zeitspanne an, in der ein Kennwort verwendet werden kann, bevor ein neues Kennwort erwartet wird.
Kennwortchronik	Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert **5** eingegeben, werden die letzten fünf Kennwörter des Benutzers gespeichert.
Min. Kennwortstärke	Angabe, wie sicher ein Kennwort sein muss. Je höher die Kennwortstärke, desto sicherer ist das Kennwort. Mit dem Wert **0** wird die Kennwortstärke nicht geprüft. Die Werte **1**, **2**, **3** und **4** geben die erforderliche Komplexität des Kennwortes an. Dabei stellt der Wert **1** die geringsten Anforderungen an die Komplexität eines Kennwortes. Der Wert **4** fordert die höchste Komplexität.
Namensbestandteile unzulässig	Angabe, ob Namensbestandteile im Kennwort zulässig oder unzulässig sind. Ist die Option aktiviert, sind Namensbestandteile in Kennwörtern nicht zulässig. Es werden die Werte der Spalten berücksichtigt, für welche die Option **Enthält Namensbestandteile für die Kennwortprüfung** aktiviert ist. Die Option passen Sie im Designer an der Spaltendefinition an. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Zeichenklassen für Kennwörter

Auf dem Tabreiter **Zeichenklassen** legen Sie fest, welche Zeichen für ein Kennwort zulässig sind.

Tabelle 21: Zeichenklassen für Kennwörter

Eigenschaft	Bedeutung
Min. Anzahl Buchstaben	Angabe, wie viele alphabetische Zeichen ein Kennwort mindestens enthalten muss.
Min. Anzahl Kleinbuchstaben	Angabe, wie viele Kleinbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Großbuchstaben	Angabe, wie viele Großbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Ziffern	Angabe, wie viele Ziffern ein Kennwort mindestens enthalten muss.
Min. Anzahl Sonderzeichen	Angabe, wie viele Sonderzeichen ein Kennwort mindestens enthalten muss.
Zulässige Sonderzeichen	Liste zulässiger Sonderzeichen.
Max. identische Zeichen insgesamt	Maximale Anzahl identischer Zeichen, die insgesamt im Kennwort vorkommen dürfen.
Max. identische Zeichen aufeinanderfolgend	Maximale Anzahl identischer Zeichen, die nacheinander wiederholt werden können.
Unzulässige Sonderzeichen	Liste unzulässiger Sonderzeichen.
Keine Kleinbuchstaben erzeugen	Angabe, ob ein generiertes Kennwort Kleinbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keinen Großbuchstaben erzeugen	Angabe, ob ein generiertes Kennwort Großbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keine Ziffern erzeugen	Angabe, ob ein generiertes Kennwort Ziffern enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keine Sonderzeichen erzeugen	Angabe, ob ein generiertes Kennwort Sonderzeichen enthalten darf. Ist die Option aktiviert, sind nur Buchstaben, Zahlen und Leerzeichen in Kennwörtern erlaubt. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.

Kundenspezifische Skripte für Kennwortanforderungen

Kundenspezifische Skripte zum Prüfen und Generieren von Kennwörtern können Sie einsetzen, wenn die Anforderungen an Kennwörter mit den vorhandenen Einstellmöglichkeiten nicht abgebildet werden können. Skripte werden zusätzlich zu den anderen Einstellungen angewendet.

Detaillierte Informationen zum Thema

- Skript zum Prüfen eines Kennwortes auf Seite 91
- Skript zum Generieren eines Kennwortes auf Seite 92

Skript zum Prüfen eines Kennwortes

Ein Prüfskript können Sie einsetzen, wenn zusätzliche Richtlinien beim Prüfen eines Kennwortes angewendet werden sollen, die nicht mit den vorhandenen Einstellmöglichkeiten abgebildet werden können.

Syntax für Prüfskripte

```
Public Sub CCC_CustomPwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
```

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Kennwort, das zu prüfen ist

TIPP: Um das Basisobjekt zu verwenden, nutzen Sie die Eigenschaft `Entity` der `PasswordPolicy`-Klasse.

Beispiel für ein Skript zum Prüfen eines Kennwortes

Ein Kennwort in darf nicht mit **?** oder **!** beginnen. Das Kennwort darf nicht mit drei identischen Zeichen beginnen. Das Skript prüft ein gegebenes Kennwort auf Zulässigkeit.

```
Public Sub CCC_PwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            Throw New Exception(#LD("Password can't start with '?' or '!'")#)
        End If
    End If
```

```
    If pwd.Length>2
        If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
            Throw New Exception(#LD("Invalid character sequence in password")#)
        End If
    End If
End Sub
```

Um ein kundenspezifisches Skript zum Prüfen eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
    b. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Tragen Sie auf dem Tabreiter **Skripte** im Eingabefeld **Prüfskript** den Namen des Skriptes ein, das zum Prüfen eines Kennwortes verwendet wird.
    e. Speichern Sie die Änderungen.

Verwandte Themen

- Skript zum Generieren eines Kennwortes auf Seite 92

Skript zum Generieren eines Kennwortes

Ein Generierungsskript können Sie einsetzen, wenn zusätzliche Richtlinien beim Generieren eines Zufallskennwortes angewendet werden sollen, die nicht mit den vorhandenen Einstellmöglichkeiten abgebildet werden können.

Syntax für Generierungsskripte

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)
```

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Generiertes Kennwort

TIPP: Um das Basisobjekt zu verwenden, nutzen Sie die Eigenschaft `Entity` der `PasswordPolicy`-Klasse.

Beispiel für ein Skript zum Generieren eines Kennwortes

Das Skript ersetzt in Zufallskennwörtern die unzulässigen Zeichen **?** und **!** zu Beginn eines Kennwortes mit **_**.

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)

    Dim pwd = spwd.ToInsecureArray()

    ' replace invalid characters at first position

    If pwd.Length>0

        If pwd(0)="?" Or pwd(0)="!"

            spwd.SetAt(0, CChar("_"))

        End If

    End If

End Sub
```

Um ein kundenspezifisches Skript zum Generieren eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
    b. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Tragen Sie auf dem Tabreiter **Skripte** im Eingabefeld **Generierungsskript** den Namen des Skriptes ein, das zum Generieren eines Kennwortes verwendet wird.
    e. Speichern Sie die Änderungen.

Verwandte Themen

- Skript zum Prüfen eines Kennwortes auf Seite 91

Ausschlussliste für Kennwörter bearbeiten

Um bestimmte Begriffe im Kennwort zu verbieten, nehmen Sie den Begriff in die Ausschlussliste auf.

HINWEIS: Die Ausschlussliste ist global für alle Kennwortrichtlinien gültig.

Um einen Begriff in die Ausschlussliste aufzunehmen

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | Kennwort Ausschlussliste**.
2. Erstellen Sie einen neuen Eintrag über den Menüeintrag **Objekt | Neu** und erfassen Sie den auszuschließenden Begriff.
3. Speichern Sie die Änderungen.

Kennwörter prüfen

Beim Prüfen eines Kennwortes werden alle definierten Einstellungen der Kennwortrichtlinie, kundenspezifische Skripte sowie die Ausschlussliste für Kennwörter berücksichtigt.

Um zu prüfen, ob ein Kennwort der Kennwortrichtlinie entspricht

1. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Test**.
5. Wählen Sie in der Auswahlliste **Basisobjekt für den Test** die Tabelle und das Objekt für die Prüfung.
6. Geben Sie im Eingabefeld **Kennwort überprüfen** das Kennwort ein.

   Neben dem Eingabefeld wird angezeigt, ob das Kennwort gültig ist.

Generieren von Kennwörtern testen

Beim Generieren eines Kennwortes werden alle definierten Einstellungen der Kennwortrichtlinie, kundenspezifische Skripte sowie die Ausschlussliste für Kennwörter berücksichtigt.

Um ein Kennwort zu generieren, das der Kennwortrichtlinie entspricht

1. Wählen Sie im Manager die Kategorie **G Suite | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Test**.
5. Klicken Sie auf die Schaltfläche **Generieren**.

   Das generierte Kennwort wird angezeigt.

Initiales Kennwort für neue G Suite Benutzerkonten

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

- Erstellen Sie Benutzerkonten manuell und tragen Sie in den Stammdaten der Benutzerkonten ein Kennwort ein.
- Vergeben Sie beim Erstellen von Benutzerkonten ein zufällig generiertes initiales Kennwort.
  - Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | GoogleApps | Accounts | InitialRandomPassword**.
  - Verwenden Sie zielsystemspezifische Kennwortrichtlinien und definieren Sie in den Kennwortrichtlinien die Zeichenklassen, die das Kennwort enthalten muss.
  - Legen Sie fest, an welche Person das initiale Kennwort per E-Mail versendet wird.
- Verwenden Sie das zentrale Kennwort der Person. Das zentrale Kennwort der zugeordneten Person wird auf das Kennwort des Benutzerkontos abgebildet. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- Kennwortrichtlinien für G Suite Benutzerkonten auf Seite 83
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 95

E-Mail-Benachrichtigungen über Anmeldeinformationen

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

Um Benachrichtigungen zu nutzen, sind folgende Voraussetzungen zu erfüllen:

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

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

Um die initialen Anmeldeinformationen per E-Mail zu versenden

1. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | GoogleApps | Accounts | InitialRandomPassword**.
2. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo** und erfassen Sie als Wert den Empfänger der Benachrichtigung.

   Ist kein Empfänger ermittelbar, dann wird die E-Mail an die im Konfigurationsparameter **TargetSystem | GoogleApps | DefaultAddress** hinterlegte Adresse versandt.
3. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName**.

   Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Person - Erstellung neues Benutzerkonto** versendet. Die Benachrichtigung enthält den Namen des Benutzerkontos.
4. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword**.

   Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Person - Initiales Kennwort für neues Benutzerkonto** versendet. Die Benachrichtigung enthält das initiale Kennwort für das Benutzerkonto.

HINWEIS: Um andere als die Standardmailvorlagen für diese Benachrichtigungen zu nutzen, ändern Sie die Werte der Konfigurationsparameter.

5

Managen von G Suite Berechtigungszuweisungen

In einer G Suite können die Nutzer verschiedene Berechtigungen haben, die folgendermaßen im One Identity Manager abgebildet werden:

- Berechtigung zur Anmeldung an der G Suite

  Tabelle: **G Suite Produkte und SKUs** (GAPPaSku)
- Administrative Berechtigungen

  Tabelle: **G Suite Admin-Rollen-Zuordnungen** (GAPOrgAdminRole)
- Berechtigung zur Nutzung von G Suite Gruppen

  Tabelle: **G Suite Gruppen** (GAPGroup)

Als Berechtigungszuweisungen werden die Zuweisungen der verschiedenen Berechtigungen an Benutzerkonten bezeichnet. Dazu gehören:

- G Suite Benutzerkonten: Zuweisungen an Produkte und SKUs (Tabelle GAPUserInPaSku)
- G Suite Benutzerkonten: Zuweisungen an Gruppen (Tabelle GAPUserInGroup)
- G Suite Gruppen: Zuweisungen an Kunden (Tabelle GAPCustomerInGroup)

Zuweisen von G Suite Berechtigungen an Benutzerkonten im One Identity Manager

Im One Identity Manager können G Suite Berechtigungen direkt oder indirekt an Personen zugewiesen werden.

Bei der indirekten Zuweisung werden Personen und Berechtigungen in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der Berechtigungen, die einer Person zugewiesen ist. Wenn die

Person ein G Suite Benutzerkonto besitzt, dann erhält dieses Benutzerkonto die Berechtigungen.

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

Über Systemrollen können Berechtigungen zusammengefasst und als Paket an Personen zugewiesen werden. Sie können Systemrollen erstellen, die ausschließlich G Suite Berechtigungen enthalten. Ebenso können in einer Systemrolle Systemberechtigungen aus unterschiedlichen Zielsystemen zusammengefasst werden.

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

Voraussetzungen

- Für Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen ist die Zuweisung von Personen, G Suite Produkten und SKUs und G Suite Gruppen erlaubt.
- Die Benutzerkonten sind mit der Option **Berechtigungen erbbar** gekennzeichnet.
- Die Benutzerkonten sind über die Spalte `UID_Person` (**Person**) mit einer Person verbunden.
- Benutzerkonten und Berechtigungen gehören zur selben Kunden-Umgebung.

Ausführliche Informationen finden Sie in den folgenden Handbüchern.

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

Detaillierte Informationen zum Thema

- G Suite Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 99
- G Suite Berechtigungen an Geschäftsrollen zuweisen auf Seite 100
- G Suite Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 104
- G Suite Berechtigungen in Systemrollen aufnehmen auf Seite 101

- G Suite Berechtigungen in den IT Shop aufnehmen auf Seite 102
- G Suite Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 104
- G Suite Gruppen direkt an einen Kunden zuweisen auf Seite 105
- G Suite Kunden direkt an eine Gruppe zuweisen auf Seite 105

G Suite Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie Gruppen und Produkte und SKUs an Abteilungen, Kostenstellen oder Standorte zu, damit sie über diese Organisationen an Benutzerkonten zugewiesen werden.

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

1. Wählen Sie eine der folgenden Kategorien.
   - **G Suite | Gruppen**
   - **G Suite | Produkte und SKUs**
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

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

   Um eine Zuweisung zu entfernen
   - Wählen Sie die Organisation und doppelklicken Sie .
5. Speichern Sie die Änderungen.

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

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

   - ODER -

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

   - ODER -

   Wählen Sie die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.

3. Wählen Sie eine der folgenden Aufgaben.
    - **G Suite Gruppen zuweisen**
    - **G Suite Produkte und SKUs zuweisen**
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungen zu.

    - ODER -

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

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer G Suite auf Seite 10

G Suite Berechtigungen an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie Berechtigungen an Geschäftsrollen zu, damit sie über diese Geschäftsrollen an Benutzerkonten zugewiesen werden.

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

1. Wählen Sie eine der folgenden Kategorien.
    - **G Suite | Gruppen**
    - **G Suite | Produkte und SKUs**
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

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

    Um eine Zuweisung zu entfernen

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

Um Berechtigungen an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)

1. Wählen Sie die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.

3. Wählen Sie eine der folgenden Aufgaben.
    - **G Suite Gruppen zuweisen**
    - **G Suite Produkte und SKUs zuweisen**
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungen zu.

    - ODER -

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

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer G Suite auf Seite 10

G Suite Berechtigungen in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

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

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

Um eine Berechtigung an Systemrollen zuzuweisen

1. Wählen Sie eine der folgenden Kategorien.
    - **G Suite | Gruppen**
    - **G Suite | Produkte und SKUs**
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

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

    Um eine Zuweisung zu entfernen

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

G Suite Berechtigungen in den IT Shop aufnehmen

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

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

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

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

Um eine Berechtigung in den IT Shop aufzunehmen

1. Wählen Sie im Manager eine der folgenden Kategorien (bei nicht-rollenbasierter Anmeldung).
   - **G Suite | Gruppen**
   - **G Suite | Produkte und SKUs**

   - ODER -

   Wählen Sie im Manager eine der folgenden Kategorien (bei rollenbasierter Anmeldung).
   - **Berechtigungen | G Suite Gruppen**
   - **Berechtigungen | G Suite Produkte und SKUs**
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigung an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Berechtigung aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager eine der folgenden Kategorien (bei nicht-rollenbasierter Anmeldung).

- **G Suite | Gruppen**
- **G Suite | Produkte und SKUs**

- ODER -

Wählen Sie im Manager eine der folgenden Kategorien (bei rollenbasierter Anmeldung).

- **Berechtigungen | G Suite Gruppen**
- **Berechtigungen | G Suite Produkte und SKUs**

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

Um eine Berechtigung aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager eine der folgenden Kategorien (bei nicht-rollenbasierter Anmeldung).
   - **G Suite | Gruppen**
   - **G Suite | Produkte und SKUs**

   - ODER -

   Wählen Sie im Manager eine der folgenden Kategorien (bei rollenbasierter Anmeldung).
   - **Berechtigungen | G Suite Gruppen**
   - **Berechtigungen | G Suite Produkte und SKUs**
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

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

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

Verwandte Themen

- Allgemeine Stammdaten für G Suite Gruppen auf Seite 136
- Allgemeine Stammdaten für G Suite Produkte und SKUs auf Seite 144
- One Identity Manager Benutzer für die Verwaltung einer G Suite auf Seite 10

G Suite Benutzerkonten direkt an eine Berechtigung zuweisen

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

Um eine Berechtigung direkt an Benutzerkonten zuzuweisen

1. Wählen Sie eine der folgenden Kategorien.
    - **G Suite | Gruppen**
    - **G Suite | Produkte und SKUs**
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Mitglieder zuweisen**.
4. Wählen Sie den Tabreiter **Benutzer**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

G Suite Berechtigungen direkt an ein Benutzerkonto zuweisen

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

Um Berechtigungen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie die Kategorie **G Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie eine der folgenden Aufgaben.
    - **Gruppen zuweisen**
    - **Produkte und SKUs zuweisen**
    - **Admin-Rollen-Zuordnungen zuweisen**
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungen zu.

   - ODER -

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

G Suite Gruppen direkt an einen Kunden zuweisen

Um alle Benutzerkonten einer Kunden-Umgebung als Mitglieder in G Suite Gruppen aufzunehmen, weisen Sie die Gruppen direkt an den G Suite Kunden zu. Bei der Vererbungsberechnung wird für alle Benutzerkonten der Kunden-Umgebung ein Eintrag in der Tabelle GAPUserInGroup erstellt. Die Herkunft der Zuweisung ist in der Spalte XOrigin mit dem Wert **16** gekennzeichnet.

Um Gruppen direkt an einen Kunden zuzuweisen

1. Wählen Sie die Kategorie **G Suite | G Suite Kunden**.
2. Wählen Sie in der Ergebnisliste den Kunden.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

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

Verwandte Themen

- Besonderheiten bei der Zuweisung von G Suite Gruppen auf Seite 181

G Suite Kunden direkt an eine Gruppe zuweisen

Um alle Benutzerkonten einer Kunden-Umgebung als Mitglieder in eine G Suite Gruppe aufzunehmen, weisen Sie den G Suite Kunden direkt an die Gruppe zu. Bei der Vererbungsberechnung wird für alle Benutzerkonten der Kunden-Umgebung ein Eintrag in der Tabelle GAPUserInGroup erstellt. Die Herkunft der Zuweisung ist in der Spalte XOrigin mit dem Wert **16** gekennzeichnet.

Um Kunden direkt an eine Gruppe zuzuweisen

1. Wählen Sie die Kategorie **G Suite | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **G Suite Kunden zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kunden zu.

   - ODER -

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

Verwandte Themen

- Besonderheiten bei der Zuweisung von G Suite Gruppen auf Seite 181

Wirksamkeit von G Suite Berechtigungszuweisungen

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

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

HINWEIS:

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

Die Wirksamkeit der Zuweisungen wird in den Tabellen GAPUserInGroup und GAPBaseTreeHasGroup über die Spalte XIsInEffect abgebildet.

Beispiel für die Wirksamkeit von Gruppenmitgliedschaften

- In einer Kunden-Umgebung sind die Gruppen A, B und C definiert.
- Gruppe A wird über die Abteilung "Marketing", Gruppe B über die Abteilung "Finanzen" und Gruppe C wird über die Geschäftsrolle "Kontrollgruppe" zugewiesen.

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

Durch geeignete Maßnahmen soll verhindert werden, dass eine Person gleichzeitig die Berechtigungen der Gruppe A und der Gruppe B erhält. Das heißt, die Gruppen A und B schließen sich aus. Ein Benutzer, der Mitglied der Gruppe C ist, darf ebenfalls nicht gleichzeitig Mitglied der Gruppe B sein. Das heißt, die Gruppen B und C schließen sich aus.

Tabelle 22: Festlegen der ausgeschlossenen Gruppen (Tabelle `GAPGroupExclusion`)

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

Tabelle 23: Wirksame Zuweisungen

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

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

Für Jenny Basset sind die Gruppen A und C wirksam, da zwischen beiden Gruppen kein Ausschluss definiert wurde. Soll das verhindert werden, definieren Sie einen weiteren Ausschluss für die Gruppe C.

Tabelle 24: Ausgeschlossene Gruppen und wirksame Zuweisungen

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

Voraussetzungen

- Der Konfigurationsparameter **QER | Structures | Inherite | GroupExclusion** ist aktiviert.
- Sich ausschließende Gruppen gehören zur selben Kunden-Umgebung.

Um Gruppen auszuschließen

1. Wählen Sie im Manager die Kategorie **G Suite | Gruppen**.
2. Wählen Sie in der Ergebnisliste eine Gruppe.
3. Wählen Sie die Aufgabe **Gruppen ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu, die sich mit der gewählten Gruppe ausschließen.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Vererbung von G Suite Berechtigungen anhand von Kategorien

Im One Identity Manager können Berechtigungen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Berechtigungen und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält verschiedene Tabellen. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In den übrigen Tabellen geben Sie Ihre Kategorien für die Berechtigungen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 31**.

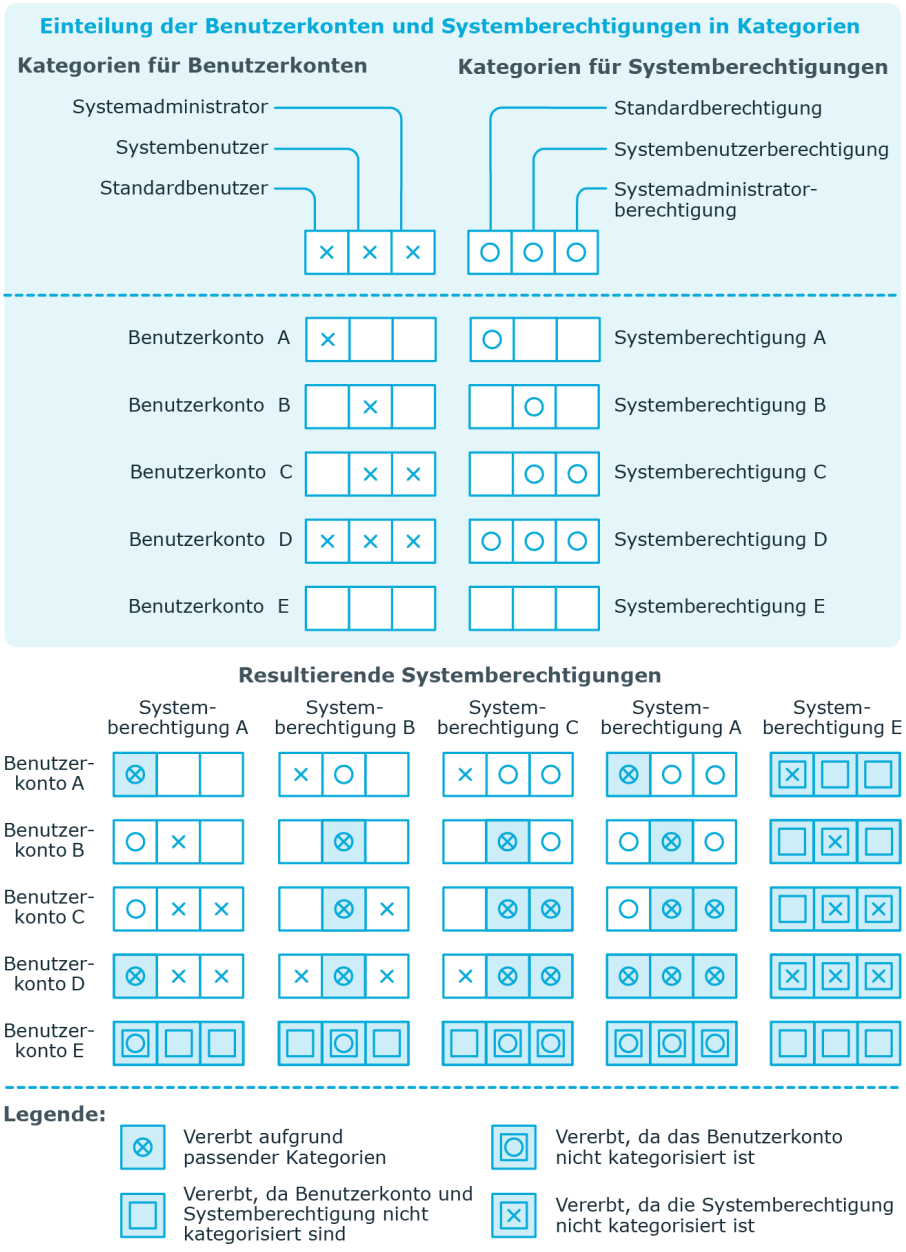
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Berechtigung kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Berechtigung überein, wird die Berechtigung an das Benutzerkonto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

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

Tabelle 25: Beispiele für Kategorien

Kategorieposition	Kategorien für Benutzerkonten	Kategorien für Berechtigungen
1	Standardbenutzer	Standardgruppe
2	Administrator	Administratorgruppe

Abbildung 2: Beispiel für die Vererbung über Kategorien



Um die Vererbung über Kategorien zu nutzen

- Definieren Sie am G Suite Kunden die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Gruppen sowie den Produkten und SKUs über ihre Stammdaten zu.

Verwandte Themen

- Kategorien für die Vererbung von G Suite Berechtigungen definieren auf Seite 115
- Allgemeine Stammdaten für G Suite Benutzerkonten auf Seite 120
- Allgemeine Stammdaten für G Suite Gruppen auf Seite 136
- Allgemeine Stammdaten für G Suite Produkte und SKUs auf Seite 144

Übersicht aller Zuweisungen

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

Beispiele

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

Um detaillierte Informationen über Zuweisungen anzuzeigen

- Um den Bericht anzuzeigen, wählen Sie in der Navigation oder in der Ergebnisliste das Basisobjekt und wählen Sie den Bericht **Übersicht aller Zuweisungen**.
- Wählen Sie über die Schaltfläche **Verwendet von** in der Symbolleiste des Berichtes die Rollenklasse, für die Sie ermitteln möchten, ob es Rollen gibt, in denen sich Personen mit dem ausgewählten Basisobjekt befinden.

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

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

Abbildung 3: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 26: Bedeutung der Symbole in der Symbolleiste des Berichts

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

Abbilden von G Suite Objekten im One Identity Manager

Mit dem One Identity Manager verwalten Sie alle Objekte der G Suite, die für die Optimierung der Zugriffssteuerung im Zielsystem benötigt werden. Diese Objekte werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können im Manager angezeigt oder bearbeitet werden.

G Suite Kunden

Das Zielsystem der Synchronisation einer G Suite ist die primäre Domain eines G Suite Kunden. G Suite Kunden werden als Basisobjekte der Synchronisation im One Identity Manager angelegt. Sie werden genutzt, um Provisionierungsprozesse, die automatische Zuordnung von Personen zu Benutzerkonten und die Vererbung von G Suite Berechtigungen an Benutzerkonten zu konfigurieren.

G Suite Kunden erstellen

HINWEIS: Die Einrichtung der G Suite Kunden in der One Identity Manager-Datenbank übernimmt der Synchronization Editor. Falls erforderlich, können Kunden auch im Manager erstellt werden.

Um einen Kunden einzurichten

1. Wählen Sie im Manager die Kategorie **G Suite | G Suite Kunden**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten für den Kunden.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für G Suite Kunden auf Seite 113
- Adressdaten von G Suite Kunden auf Seite 115
- Kategorien für die Vererbung von G Suite Berechtigungen definieren auf Seite 115
- Stammdaten für G Suite Kunden bearbeiten auf Seite 113

Stammdaten für G Suite Kunden bearbeiten

Um die Stammdaten eines Kunden zu bearbeiten

1. Wählen Sie im Manager die Kategorie **G Suite | G Suite Kunden**.
2. Wählen Sie in der Ergebnisliste den Kunden.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für den Kunden.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für G Suite Kunden auf Seite 113
- Adressdaten von G Suite Kunden auf Seite 115
- Kategorien für die Vererbung von G Suite Berechtigungen definieren auf Seite 115
- G Suite Kunden erstellen auf Seite 112

Allgemeine Stammdaten für G Suite Kunden

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

Tabelle 27: Allgemeine Stammdaten eines G Suite Kunden

Eigenschaft	Beschreibung
G Suite Kunde	Eindeutige Kennung des G Suite Kunden.
Primäre Domain des Kunden	Name der primären Domain des Kunden.
Kunde erstellt am	Zeitpunkt, an dem die Kunden-Umgebung erstellt wurde.
Alternative E-Mail-Adresse	Zweite E-Mail-Adresse des Kunden. Diese E-Mail-Adresse darf nicht in der Domain des Kunden sein.

Eigenschaft	Beschreibung
Telefonnummer	Telefonnummer des Kunden im E.164 Format.
Land	Eindeutige Kennung des Landes.
Sprachkultur	Name der Sprachkultur.
Kontendefinition (initial)	Initiale Kontendefinition zur Erzeugung von Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für diesen Kunden die automatische Zuordnung von Personen zu Benutzerkonten genutzt wird und dabei bereits verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen sollen. Es wird der Standardautomatisierungsgrad der Kontendefinition angewendet. Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen Synchronisation der Fall.
Zielsystemverantwortliche	Anwendungsrolle, in der die Zielsystemverantwortlichen des Kunden festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte des Kunden, dem sie zugeordnet sind. Jedem Kunden können andere Zielsystemverantwortliche zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle aus, deren Mitglieder verantwortlich für die Administration dieses Kunden sind. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.
Synchronisiert durch	Art der Synchronisation, über welche die Daten zwischen dem Kunden und dem One Identity Manager ausgetauscht werden. Sobald Objekte für diesen Kunden im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden. Beim Erstellen eines Kunden mit dem Synchronization Editor wird **One Identity Manager** verwendet.

Tabelle 28: Zulässige Werte

Wert	Synchronisation durch	Provisionierung durch
One Identity Manager	G Suite Konnektor	G Suite Konnektor
Keine Synchronisation	keine	keine

Eigenschaft	Beschreibung
	HINWEIS: Wenn Sie **Keine Synchronisation** festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.

Verwandte Themen

- Kontendefinitionen an Zielsysteme zuweisen auf Seite 66
- Kontendefinitionen für G Suite Benutzerkonten auf Seite 51
- Automatische Zuordnung von Personen zu G Suite Benutzerkonten auf Seite 69
- Zielsystemverantwortliche für Kunden-Umgebungen auf Seite 167

Adressdaten von G Suite Kunden

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

Tabelle 29: Adressdaten eines G Suite Kunden

Eigenschaft	Beschreibung
Name der Organisation	Name der Organisation für die Postadresse des Kunden.
Name der Kontaktperson	Kontaktperson des Kunden.
Adresszeile 1-3	Postadresse des Kunden.
Region	Region der Postadresse.
Ort	Ort der Postadresse.
Postleitzahl	Postleitzahl der Postadresse.

Kategorien für die Vererbung von G Suite Berechtigungen definieren

Im One Identity Manager können Berechtigungen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Berechtigungen und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält verschiedene Tabellen. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In den übrigen Tabellen geben Sie Ihre Kategorien für die Berechtigungen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 31**.

Um Kategorien zu definieren

1. Wählen Sie im Manager in der Kategorie **G Suite | Kunden-Umgebungen** die Kunden-Umgebung.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wechseln Sie auf den Tabreiter **Abbildungsvorschrift Kategorien**.
4. Erweitern Sie den jeweiligen Basisknoten einer Tabelle.
5. Aktivieren Sie die Kategorie per Maus-Doppelklick auf das Symbol .
6. Tragen Sie eine beliebige Benennung der Kategorie für Benutzerkonten und Gruppen sowie Produkte und SKUs in der verwendeten Anmeldesprache ein.
7. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Vererbung von G Suite Berechtigungen anhand von Kategorien auf Seite 108

Zusätzliche Aufgaben zur Verwaltung von G Suite Kunden

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Aufgabe	Thema
Überblick über den G Suite Kunden	Überblick über einen G Suite Kunden auf Seite 116
Gruppen zuweisen	G Suite Gruppen direkt an einen Kunden zuweisen auf Seite 105
Suchkriterien für die Personenzuordnung definieren	Suchkriterien für die automatische Personenzuordnung bearbeiten auf Seite 71
Synchronisationsprojekt bearbeiten	Synchronisationsprojekt für einen G Suite Kunden bearbeiten auf Seite 117
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 44

Überblick über einen G Suite Kunden

Um einen Überblick über einen G Suite Kunden zu erhalten

1. Wählen Sie im Manager die Kategorie **G Suite | G Suite Kunden**.
2. Wählen Sie in der Ergebnisliste den Kunden.

3. Wählen Sie die Aufgabe **Überblick über den G Suite Kunden**.

Synchronisationsprojekt für einen G Suite Kunden bearbeiten

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

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

Um ein bestehendes Synchronisationsprojekt im Synchronization Editor zu öffnen

1. Wählen Sie im Manager die Kategorie **G Suite | G Suite Kunden**.
2. Wählen Sie in der Ergebnisliste den Kunden.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten**.

Verwandte Themen

- Anpassen der Synchronisationskonfiguration für G Suite-Umgebungen auf Seite 28

G Suite Benutzerkonten

Mit dem One Identity Manager verwalten Sie die Nutzer einer G Suite. Die Nutzerdaten der registrierten Nutzer werden als Benutzerkonten im One Identity Manager abgebildet. Über die Benutzerkonten verwalten Sie die Berechtigungen der Nutzer, wie beispielsweise die Mitgliedschaft in G Suite Gruppen oder administrative Berechtigungen.

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

HINWEIS: Um Benutzerkonten für die Personen eines Unternehmens einzurichten, wird der Einsatz von Kontendefinitionen empfohlen. Einige der nachfolgend beschriebenen Stammdaten werden dabei über Bildungsregeln aus den Personenstammdaten gebildet.

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

Verwandte Themen

- Managen von G Suite Benutzerkonten und Personen auf Seite 50
- Kontendefinitionen für G Suite Benutzerkonten auf Seite 51
- Standardprojektvorlage für eine G Suite auf Seite 175
- Stammdaten für G Suite Benutzerkonten bearbeiten auf Seite 119
- Managen von G Suite Berechtigungszuweisungen auf Seite 97

G Suite Benutzerkonten erstellen

Um ein Benutzerkonto zu erstellen

1. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

An Benutzerkonten können verschiedene Kommunikationsdaten und organisatorische Daten zugewiesen werden, wie E-Mail-Adressen, Websites, Informationen über die Organisation des Nutzers oder Beziehungen zu anderen Nutzern.

Um Kommunikationsdaten an ein Benutzerkonto zuzuweisen

1. Auf dem Stammdatenformular wählen Sie den gewünschten Tabreiter.
2. Klicken Sie **Hinzufügen**.

   Es wird eine neue Zeile in die Tabelle eingefügt.
3. Markieren Sie diese Zeile und bearbeiten Sie die Stammdaten.
4. Speichern Sie die Änderungen.

Um Kommunikationsdaten zu bearbeiten

1. Auf dem Stammdatenformular wählen Sie den gewünschten Tabreiter.
2. Wählen Sie in der Tabelle die Zeile, die Sie bearbeiten möchten.
3. Bearbeiten Sie die Stammdaten.
4. Speichern Sie die Änderungen.

Um die Zuweisung von Kommunikationsdaten zu entfernen

1. Auf dem Stammdatenformular wählen Sie den gewünschten Tabreiter.
2. Wählen Sie in der Tabelle die Zeile, die Sie entfernen möchten.
3. Klicken Sie **Entfernen**.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für G Suite Benutzerkonten auf Seite 120
- Kennwortdaten für G Suite Benutzerkonten auf Seite 124
- Telefonnummern für G Suite Benutzerkonten auf Seite 125
- Adressen für G Suite Benutzerkonten auf Seite 125
- E-Mail-Adressen für G Suite Benutzerkonten auf Seite 126
- Externe IDs für G Suite Benutzerkonten auf Seite 126
- Instant Messenger Daten für G Suite Benutzerkonten auf Seite 127
- Nutzerdetails für G Suite Benutzerkonten auf Seite 128
- Beziehungen von G Suite Benutzerkonten auf Seite 128
- Websites von G Suite Benutzerkonten auf Seite 129

Verwandte Themen

- Stammdaten für G Suite Benutzerkonten bearbeiten
- G Suite Benutzerkonten löschen und wiederherstellen

Stammdaten für G Suite Benutzerkonten bearbeiten

Um die Stammdaten eines Benutzerkontos zu bearbeiten

1. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

An Benutzerkonten können verschiedene Kommunikationsdaten und organisatorische Daten zugewiesen werden, wie E-Mail-Adressen, Websites, Informationen über die Organisation des Nutzers oder Beziehungen zu anderen Nutzern.

Um Kommunikationsdaten an ein Benutzerkonto zuzuweisen

1. Auf dem Stammdatenformular wählen Sie den gewünschten Tabreiter.
2. Klicken Sie **Hinzufügen**.

   Es wird eine neue Zeile in die Tabelle eingefügt.
3. Markieren Sie diese Zeile und bearbeiten Sie die Stammdaten.
4. Speichern Sie die Änderungen.

Um Kommunikationsdaten zu bearbeiten

1. Auf dem Stammdatenformular wählen Sie den gewünschten Tabreiter.
2. Wählen Sie in der Tabelle die Zeile, die Sie bearbeiten möchten.
3. Bearbeiten Sie die Stammdaten.
4. Speichern Sie die Änderungen.

Um die Zuweisung von Kommunikationsdaten zu entfernen

1. Auf dem Stammdatenformular wählen Sie den gewünschten Tabreiter.
2. Wählen Sie in der Tabelle die Zeile, die Sie entfernen möchten.
3. Klicken Sie **Entfernen**.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für G Suite Benutzerkonten auf Seite 120
- Kennwortdaten für G Suite Benutzerkonten auf Seite 124
- Telefonnummern für G Suite Benutzerkonten auf Seite 125
- Adressen für G Suite Benutzerkonten auf Seite 125
- E-Mail-Adressen für G Suite Benutzerkonten auf Seite 126
- Externe IDs für G Suite Benutzerkonten auf Seite 126
- Instant Messenger Daten für G Suite Benutzerkonten auf Seite 127
- Nutzerdetails für G Suite Benutzerkonten auf Seite 128
- Beziehungen von G Suite Benutzerkonten auf Seite 128
- Websites von G Suite Benutzerkonten auf Seite 129

Verwandte Themen

- G Suite Benutzerkonten erstellen
- G Suite Benutzerkonten löschen und wiederherstellen
- G Suite Benutzerkonten sperren

Allgemeine Stammdaten für G Suite Benutzerkonten

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

Tabelle 30: Allgemeine Stammdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Person	Person, die das Benutzerkonto verwendet. Wurde das Benutzerkonto über eine Kontendefinition erzeugt, ist die Person bereits eingetragen. Wenn Sie das Benutzerkonto manuell erstellen, können Sie die Person aus der Auswahlliste wählen. Wenn Sie die automatische Personenzuordnung nutzen, wird beim Speichern des Benutzerkontos eine zugehörige Person gesucht und in das Benutzerkonto übernommen. Für ein Benutzerkonto mit einer Identität vom Typ **Organisatorische Identität**, **Persönliche Administratoridentität**, **Zusatzidentität**, **Gruppenidentität** oder **Dienstidentität** können Sie eine neue Person erstellen. Klicken Sie dafür neben dem Eingabefeld und erfassen Sie die erforderlichen Personenstammdaten. Die Pflichteingaben sind abhängig vom gewählten Identitätstyp. HINWEIS: Um mit Identitäten für Benutzerkonten zu arbeiten, benötigen die Personen ebenfalls Identitäten. Benutzerkonten, denen eine Identität zugeordnet ist, können Sie nur mit Personen verbinden, die dieselbe Identität haben.
Kontendefinition	Kontendefinition, über die das Benutzerkonto erstellt wurde. Die Kontendefinition wird benutzt, um die Stammdaten des Benutzerkontos automatisch zu befüllen und um einen Automatisierungsgrad für das Benutzerkonto festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Person und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein. HINWEIS: Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden.
Automatisierungsgrad	Automatisierungsgrad des Benutzerkontos. Wählen Sie einen Automatisierungsgrad aus der Auswahlliste. Den Automatisierungsgrad können Sie nur festlegen, wenn Sie auch eine Kontendefinition eingetragen haben. In der Auswahlliste werden alle Automatisierungsgrade der gewählten Kontendefinition angeboten.
G Suite Kunde	Kunden-Umgebung, zu der das Benutzerkonto gehört.
Eindeutige Kennung	G Suite interne ID des Benutzerkontos.
Vorname	Vorname des Nutzers.
Nachname	Nachname des Nutzers.
Primäre E-Mail-Adresse	Primäre E-Mail-Adresse des Benutzerkontos.

Eigenschaft	Beschreibung
G Suite Organisation	G Suite Organisation, zu der das Benutzerkonto gehört.
Erstellungszeit	Zeitpunkt, an dem das Benutzerkonto erstellt wurde.
Löschzeitpunkt	Zeitpunkt, an dem das Benutzerkonto gelöscht wurde. Innerhalb von fünf Tagen kann das Benutzerkonto wiederhergestellt werden.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten Berechtigungen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von G Suite Berechtigungen an das Benutzerkonto. Berechtigungen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Berechtigungen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Format für Notizen	Format für Notizen.
Notizen	Freitextfeld für zusätzliche Erläuterungen.
Gesperrt	Gibt an, ob das Benutzerkonto gesperrt ist.
Sperrgrund	Grund für die Sperre des Benutzerkontos.
Aliasse	Liste aller Alias-E-Mail-Adressen, die für das Benutzerkonto eingerichtet sind.
Nichtänderbare Aliasse	Liste aller nicht änderbaren E-Mail-Aliasse. Diese E-Mail-Adressen gehören nicht zur primären Domain oder deren Subdomains.
Identität	Typ der Identität des Benutzerkontos. Zulässige Werte sind: • **Primäre Identität**: Standardbenutzerkonto einer Person. • **Organisatorische Identität**: Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen. • **Persönliche Administratoridentität**: Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird. • **Zusatzidentität**: Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird. • **Gruppenidentität**: Benutzerkonto mit administrativen

Eigenschaft	Beschreibung
	Berechtigungen, welches von mehreren Personen genutzt wird. Weisen Sie alle Personen zu, die das Benutzerkonto nutzen. • **Dienstidentität**: Dienstkonto.
Berechtigungen erbbar	Angabe, ob das Benutzerkonto G Suite Berechtigungen über die Person erben darf. Ist die Option aktiviert, werden Berechtigungen über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt. 1. Beispiel: Eine Person mit einem G Suite Benutzerkonto ist Mitglied einer Abteilung. Dieser Abteilung ist ein G Suite Produkt und SKU zugewiesen. Wenn die Option aktiviert ist, erbt das Benutzerkonto dieses Produkt und SKU. 2. Beispiel: Eine Person mit einem G Suite Benutzerkonto bestellt eine G Suite Gruppe im IT Shop. Die Bestellung wird genehmigt und zugewiesen. Das Benutzerkonto erbt diese Gruppe nur, wenn die Option aktiviert ist.
Privilegiertes Benutzerkonto	Gibt an, ob es sich um ein privilegiertes Benutzerkonto handelt.
In globaler Adressliste anzeigen	Gibt an, ob das Benutzerkonto in der globalen Adressliste angezeigt wird.
In weißer Liste enthalten	Gibt an, ob die IP-Adresse des Benutzerkontos in der weißen Liste für E-Mails enthalten ist.
Ist Super Admin	Gibt an, ob das Benutzerkonto Super Admin Berechtigungen hat.
Delegierter Administrator	Gibt an, ob das Benutzerkonto über delegierte Admin-Berechtigungen verfügt.
G Suite Vereinbarung akzeptiert	Gibt an, ob der Nutzer sich initial an der G Suite angemeldet und die G Suite (Online) Vereinbarung akzeptiert hat.
Google Postfach ist erstellt	Gibt an, ob ein Google Postfach für das Benutzerkonto erstellt wurde.
Bestätigung in zwei Schritten ist aktiviert	Gibt an, ob die **Bestätigung in zwei Schritten** für das Benutzerkonto aktiviert ist.
Bestätigung in zwei Schritten ist erzwungen	Gibt an, ob die **Bestätigung in zwei Schritten** für das Benutzerkonto erzwungen wird.

Verwandte Themen

- Managen von G Suite Benutzerkonten und Personen auf Seite 50
- Kontendefinitionen für G Suite Benutzerkonten auf Seite 51

- Automatische Zuordnung von Personen zu G Suite Benutzerkonten auf Seite 69
- Vererbung von G Suite Berechtigungen anhand von Kategorien auf Seite 108
- G Suite Benutzerkonten sperren auf Seite 131
- Unterstützte Typen von Benutzerkonten auf Seite 76
- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 79
- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 80
- G Suite Benutzerkonten in andere Organisation verschieben auf Seite 131

Kennwortdaten für G Suite Benutzerkonten

Auf dem Tabreiter **Kennwort** vergeben Sie das Kennwort für die Anmeldung an der G Suite.

Tabelle 31: Kennwortdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Kennwort	Kennwort für das Benutzerkonto. Das zentrale Kennwort der zugeordneten Person kann auf das Kennwort des Benutzerkontos abgebildet werden. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*. Wenn Sie ein initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen. HINWEIS: Beim Prüfen eines Benutzerkennwortes werden die One Identity Manager Kennwortrichtlinien beachtet. Stellen Sie sicher, dass die Kennwortrichtlinie nicht gegen die Anforderungen des Zielsystems verstößt.
Bestätigung	Kennwortwiederholung.
Letzte Anmeldung	Zeitpunkt der letzten Anmeldung an der G Suite.
Kennwort bei der nächsten Anmeldung ändern	Gibt an, ob der Nutzer sein Kennwort bei der nächsten Anmeldung ändern muss.

Verwandte Themen

- Initiales Kennwort für neue G Suite Benutzerkonten auf Seite 95

Telefonnummern für G Suite Benutzerkonten

Auf dem Tabreiter **Telefonnummern** können Sie die Telefonnummern des Benutzerkontos bearbeiten.

Tabelle 32: Eigenschaften einer Telefonnummer

Eigenschaft	Beschreibung
Typ	Typ der Telefonnummer.
Benutzerdefinierter Typ	Benutzerdefinierter Typ der Telefonnummer. Wenn im Eingabefeld **Typ** der Wert **benutzerdefiniert** ausgewählt ist, geben Sie hier einen eigenen Telefonnummerntyp an.
Telefonnummer	Telefonnummer in beliebigem Format.
Primäre Telefon-nummer	Gibt an, ob diese Telefonnummer die primäre ist.

Verwandte Themen

- Stammdaten für G Suite Benutzerkonten bearbeiten auf Seite 119

Adressen für G Suite Benutzerkonten

Auf dem Tabreiter **Adressen** können Sie die Adressen des Benutzerkontos bearbeiten.

Tabelle 33: Eigenschaften einer Adresse

Eigenschaft	Beschreibung
Typ	Typ der Adresse.
Benutzerdefinierter Typ	Benutzerdefinierter Typ der Adresse. Wenn im Eingabefeld **Typ** der Wert **benutzerdefiniert** ausgewählt ist, geben Sie hier einen eigenen Adresstyp an.
Adresserweiterung	Adresserweiterung, beispielsweise für die Angabe einer Region.
Adresse	Vollständige Adresse.
Straße	Straße der Adresse.
Postleitzahl	Postleitzahl der Adresse.
Ort	Ort der Adresse.
Region	Region, falls benötigt.
Postfach	Postfach, wenn vorhanden.

Eigenschaft	Beschreibung
Länderkennung	Eindeutige Kennung des Landes.
Primäre Adresse	Gibt an, ob diese Adresse die primäre Adresse des Nutzers ist.
Formatierte Adresse	Gibt an, ob die Adresse formatiert bereitgestellt wurde.

Verwandte Themen

- Stammdaten für G Suite Benutzerkonten bearbeiten auf Seite 119

E-Mail-Adressen für G Suite Benutzerkonten

Auf dem Tabreiter **E-Mail-Adressen** können Sie die E-Mail-Adressen des Benutzerkontos bearbeiten.

Tabelle 34: Eigenschaften einer E-Mail-Adresse

Eigenschaft	Beschreibung
Typ	Typ der E-Mail-Adresse.
Benutzerdefinierter Typ	Benutzerdefinierter Typ der E-Mail-Adresse. Wenn im Eingabefeld **Typ** der Wert **benutzerdefiniert** ausgewählt ist, geben Sie hier einen eigenen E-Mail-Adresstyp an.
E-Mail-Adresse	Zusätzliche E-Mail-Adressen. Es kann auch die primäre E-Mail-Adresse oder ein E-Mail Alias angegeben werden.

Verwandte Themen

- Stammdaten für G Suite Benutzerkonten bearbeiten auf Seite 119

Externe IDs für G Suite Benutzerkonten

Auf dem Tabreiter **Externe IDs** können Sie die externe IDs des Benutzerkontos bearbeiten.

Tabelle 35: Eigenschaften einer externen ID

Eigenschaft	Beschreibung
Typ	Typ der externen ID.
Benutzerdefinierter	Benutzerdefinierter Typ der externen ID. Wenn im Eingabefeld **Typ**

Eigenschaft	Beschreibung
Typ	der Wert **benutzerdefiniert** ausgewählt ist, geben Sie hier einen eigenen ID-Typ an.
Externe ID	Wert der externen ID.

Verwandte Themen

- Stammdaten für G Suite Benutzerkonten bearbeiten auf Seite 119

Instant Messenger Daten für G Suite Benutzerkonten

Auf dem Tabreiter **Instant Messenger** können Sie die Instant Messenger Daten des Benutzerkontos bearbeiten.

Tabelle 36: Eigenschaften eines Instant Messengers

Eigenschaft	Beschreibung
Typ	Typ des Instant Messengers.
Benutzerdefinierter Typ	Benutzerdefinierter Typ des Instant Messengers. Wenn im Eingabefeld **Typ** der Wert **benutzerdefiniert** ausgewählt ist, geben Sie hier einen eigenen Instant-Messenger-Typ an.
Protokoll	Netzwerkprotokoll des Instant Messengers. Es kann ein benutzerdefiniertes Protokoll oder ein Standardprotokoll eingestellt werden.
Benutzerdefiniertes Protokoll	Wenn im Eingabefeld **Protokoll** der Wert **benutzerdefiniert** ausgewählt ist, geben Sie hier einen eigenen Protokolltyp an.
Netzwerk ID des Instant Messengers	Netzwerk ID des Instant Messengers.
Primärer Instant Messenger	Gibt an, ob dieser Instant Messenger der primäre ist.

Verwandte Themen

Stammdaten für G Suite Benutzerkonten bearbeiten auf Seite 119

Nutzerdetails für G Suite Benutzerkonten

Auf dem Tabreiter **Nutzerdetails** können Sie verschiedene organisatorische Daten des Benutzerkontos bearbeiten.

Tabelle 37: Eigenschaften von Nutzerdetails

Eigenschaft	Beschreibung
Typ	Typ der Organisation.
Benutzerdefinierter Typ	Benutzerdefinierter Typ der Organisation. Wenn im Eingabefeld **Typ** der Wert **unbekannt** ausgewählt ist, geben Sie hier einen eigenen Organisationstyp an.
Name der Organisation	Name der Organisation, für die Nutzerdetails gepflegt werden.
Kostenstelle	Eine Kostenstelle innerhalb der Organisation.
Abteilung	Eine Abteilung innerhalb der Organisation.
Domain	Domain, zu der die Organisation gehört.
Standort	Standort der Organisation.
Symbol	Textsymbol der Organisation, beispielsweise **GOOG** für Google.
Titel	Titel des Nutzers innerhalb der Organisation, beispielsweise **Mitglied** oder **Techniker**.
Beschreibung	Beschreibung der Nutzerdetails.
Primäre Organisation	Gibt an, ob diese Organisation die primäre Organisation des Nutzers ist.

Verwandte Themen

- Stammdaten für G Suite Benutzerkonten bearbeiten auf Seite 119

Beziehungen von G Suite Benutzerkonten

Auf dem Tabreiter **Beziehungen** können Sie die Beziehungen des Benutzerkontos bearbeiten.

Tabelle 38: Eigenschaften einer Beziehung

Eigenschaft	Beschreibung
Typ	Typ der Beziehung.

Eigenschaft	Beschreibung
Benutzerdefinierter Typ	Benutzerdefinierter Typ der Beziehung. Wenn im Eingabefeld **Typ** der Wert **benutzerdefiniert** ausgewählt ist, geben Sie hier einen eigenen Beziehungstyp an.
Beziehung	Primäre E-Mail-Adresse des Nutzers, zu dem die Beziehung besteht.

Verwandte Themen

- Stammdaten für G Suite Benutzerkonten bearbeiten auf Seite 119

Websites von G Suite Benutzerkonten

Auf dem Tabreiter **Websites** können Sie die Websites des Benutzerkontos bearbeiten.

Tabelle 39: Eigenschaften einer Website

Eigenschaft	Beschreibung
Typ	Typ oder Zweck der Website.
Benutzerdefinierter Typ	Benutzerdefinierter Typ der Website. Wenn im Eingabefeld **Typ** der Wert **benutzerdefiniert** ausgewählt ist, geben Sie hier einen eigenen Website-Typ an.
URL der Website	URL der Website.
Primäre Website	Gibt an, ob diese Website die primäre ist.

Verwandte Themen

- Stammdaten für G Suite Benutzerkonten bearbeiten auf Seite 119

Zusätzliche Aufgaben zur Verwaltung von G Suite Benutzerkonten

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Aufgabe	Thema
Überblick über das G Suite Benutzerkonto	Überblick über ein G Suite Benutzerkonto auf Seite 130
Gruppen zuweisen	G Suite Berechtigungen direkt an ein Benutzerkonto

Aufgabe	Thema
	zuweisen auf Seite 104
Produkte und SKUs zuweisen	G Suite Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 104
Admin-Rollen-Zuordnungen zuweisen	G Suite Berechtigungen direkt an ein Benutzerkonto zuweisen auf Seite 104
Zusatzeigenschaften zuweisen	Zusatzeigenschaften an ein G Suite Benutzerkonto zuweisen auf Seite 130
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 44
G Suite Organisation ändern	G Suite Benutzerkonten in andere Organisation verschieben auf Seite 131

Überblick über ein G Suite Benutzerkonto

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das G Suite Benutzerkonto**.

Zusatzeigenschaften an ein G Suite Benutzerkonto zuweisen

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

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

1. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

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

G Suite Benutzerkonten in andere Organisation verschieben

Innerhalb der Organisationshierarchie eines G Suite Kunden können Benutzerkonten in eine andere Organisation verschoben werden.

Um ein Benutzerkonto in eine andere Organisation zu verschieben

1. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Wählen Sie die Aufgabe **G Suite Organisation ändern**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **G Suite Organisation** die neuen Organisation.
6. Speichern Sie die Änderungen.

G Suite Benutzerkonten sperren

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

Szenario:

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

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

Szenario:

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

Benutzerkonten, die mit Personen verbunden sind, jedoch nicht über Kontendefinitionen verwaltet werden, werden gesperrt, wenn die Person dauerhaft oder zeitweilig deaktiviert

wird. Das Verhalten ist abhängig vom Konfigurationsparameter **QER | Person | TemporaryDeactivation**.

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

Um das Benutzerkonto bei deaktiviertem Konfigurationsparameter zu sperren

1. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Gesperrt**.
5. Speichern Sie die Änderungen.

Szenario:

- Benutzerkonten sind nicht mit Personen verbunden.

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

1. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Gesperrt**.
5. Speichern Sie die Änderungen.

Um ein Benutzerkonto zu entsperren

1. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Deaktivieren Sie auf dem Tabreiter **Allgemein** die Option **Gesperrt**.
5. Speichern Sie die Änderungen.

Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Kontendefinitionen für G Suite Benutzerkonten auf Seite 51
- Automatisierungsgrade erstellen auf Seite 56
- G Suite Benutzerkonten löschen und wiederherstellen auf Seite 133

G Suite Benutzerkonten löschen und wiederherstellen

Wird ein Benutzerkonto im One Identity Manager gelöscht, wird es zunächst zum Löschen markiert. Das Benutzerkonto wird daraufhin gesperrt. Je nach Einstellung der Löschverzögerung wird das Benutzerkonto sofort oder zu einem späteren Zeitpunkt aus der One Identity Manager-Datenbank gelöscht.

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

Um ein Benutzerkonto zu löschen, das nicht über eine Kontendefinition verwaltet wird

1. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie , um das Benutzerkonto zu löschen.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Um ein Benutzerkonto wiederherzustellen

1. Wählen Sie im Manager die Kategorie **G Suite | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste .

Konfigurieren der Löschverzögerung

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

Verwandte Themen

- G Suite Benutzerkonten sperren auf Seite 131
- Nutzerdaten an ein anderes G Suite Benutzerkonto übertragen auf Seite 134

Nutzerdaten an ein anderes G Suite Benutzerkonto übertragen

Wenn ein Benutzerkonto gelöscht wird, können verschiedene Nutzerdaten an ein anderes Benutzerkonto übertragen werden. Nach Ablauf der Löschverzögerung wird zuerst der Datentransfer in der G Suite-Umgebung initiiert. Sobald der Datentransfer im Zielsystem erfolgreich abgeschlossen ist, wird das Benutzerkonto endgültig gelöscht.

Voraussetzungen

- Der Datentransfer ist für die Kunden-Umgebung zugelassen. Dafür ist an der Zielsystemverbindung die Einstellung **Nutzerdaten vor dem Löschen transferieren** aktiviert oder die Variable `CP_TransferUserDataBeforeDelete` hat den Wert **True**.
- Der Person, mit der das gelöschte Benutzerkonto verbunden ist, ist ein Manager zugeordnet.

  - ODER -

  Das gelöschte Benutzerkonto hat eine Beziehung vom Typ **Manager**.
- Die E-Mail-Adresse des Managers gehört zur primären Domain der Kunden-Umgebung, zu der auch das gelöschte Benutzerkonto gehört.
- Für den Fall, dass auf diesem Weg keine gültige E-Mail-Adresse ermittelt werden kann, ist eine gültige Standard-E-Mail-Adresse hinterlegt. Diese ist an der Zielsystemverbindung an der Einstellung **Standard-E-Mail-Adresse für Datentransfer** oder in der Variable `CP_DefaultDataTransferTargetEmail` angegeben.

Detaillierte Informationen zum Thema

- Erweiterte Einstellungen der Systemverbindung zur G Suite auf Seite 32
- Allgemeine Stammdaten für G Suite Benutzerkonten auf Seite 120
- Beziehungen von G Suite Benutzerkonten auf Seite 128

Verwandte Themen

- G Suite Benutzerkonten löschen und wiederherstellen auf Seite 133

G Suite Gruppen

Über Gruppen können die Nutzer einer G Suite Informationen austauschen oder Besprechungen organisieren. Dabei werden die Informationen jeweils nur den Mitgliedern einer Gruppe zur Verfügung gestellt. Im One Identity Manager können Gruppen angelegt und bearbeitet und ihre Mitglieder verwaltet werden.

G Suite Gruppen erstellen

Um eine Gruppe zu erstellen

1. Wählen Sie im Manager die Kategorie **G Suite | Gruppen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für G Suite Gruppen auf Seite 136
- Zusätzliche Einstellungen für G Suite Gruppen auf Seite 137

Verwandte Themen

- Stammdaten für G Suite Gruppen erfassen auf Seite 135
- G Suite Gruppen löschen auf Seite 143

Stammdaten für G Suite Gruppen erfassen

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie im Manager die Kategorie **G Suite | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für G Suite Gruppen auf Seite 136
- Zusätzliche Einstellungen für G Suite Gruppen auf Seite 137

Verwandte Themen

- G Suite Gruppen erstellen auf Seite 135
- G Suite Gruppen löschen auf Seite 143

Allgemeine Stammdaten für G Suite Gruppen

Auf dem Tabreiter **Allgemein** bearbeiten Sie die folgenden Stammdaten.

Tabelle 40: Allgemeine Stammdaten einer Gruppe

Eigenschaft	Beschreibung
G Suite Kunde	Kunden-Umgebung, zu der die Gruppe gehört.
Gruppen-ID	Eindeutige ID der Gruppe.
Name der Gruppe	Bezeichnung der Gruppe.
E-Mail-Adresse	E-Mail-Adresse der Gruppe.
Leistungsposition	Angabe einer Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
IT Shop	Angabe, ob die Gruppe über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen. Gruppen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Vom Administrator erstellt	Gibt an, ob die Gruppe von einem Administrator erstellt wurde. Wenn die Option deaktiviert ist, wurde die Gruppe von einem Nutzer erstellt.
Aliasse	Liste weiterer E-Mail-Adressen, unter denen E-Mails an die Gruppe gesendet werden können.
Nichtänderbare Aliasse	Liste aller nicht änderbaren E-Mail-Aliasse. Diese E-Mail-Adressen gehören nicht zur primären Domain oder deren Subdomains.

Verwandte Themen

- Vererbung von G Suite Berechtigungen anhand von Kategorien auf Seite 108
- G Suite Berechtigungen in den IT Shop aufnehmen auf Seite 102

Zusätzliche Einstellungen für G Suite Gruppen

Auf dem Tabreiter **Einstellungen** bearbeiten Sie die folgenden Stammdaten.

Tabelle 41: Zusätzliche Einstellungen einer Gruppe

Eigenschaft	Beschreibung
Sprachkultur	Name der Sprachkultur, z.B. es-ES.
Externe Mitglieder zulassen	Gibt an, ob Nutzer aus anderen Domains als Mitglieder zugelassen sind. Wenn die Option aktiviert ist, legen Sie im Eingabefeld **Gruppenbeitritt** fest, welche Nutzer Mitglied werden dürfen.
Gruppenbeitritt	Wählen Sie, welche Nutzer Mitglied der Gruppe werden dürfen. Der Wert **Öffentlich** kann nur ausgewählt werden, wenn die Option **Mitglieder von außerhalb dieser Organisation zulassen** aktiviert ist.
Spamnachrichten	Wählen Sie, wie Nachrichten behandelt werden sollen, die unter Spamverdacht stehen. Mögliche Werte sind: • **Zulassen**: Ohne Moderation in der Gruppe posten. • **Moderieren**: An die Moderationswarteschlage schicken und eine Benachrichtigung an die Moderatoren senden. • **Still moderieren**: An die Moderationswarteschlage schicken, jedoch keine Benachrichtigung an die Moderatoren senden. • **Zurückweisen**: Sofort zurückweisen.
Antworten auf Beiträge	Wählen Sie, wer die Antworten auf Beiträge erhalten soll. Wenn **An eine benutzerdefinierte Adresse** ausgewählt wurde, muss im Eingabefeld **Antworten senden an** eine gültige E-Mail-Adresse angegeben werden.
Antworten senden an	E-Mail-Adresse, an die Antworten auf Beiträge gesendet werden. Es muss eine gültige E-Mail-Adresse angegeben werden, wenn im Eingabefeld **Antworten auf Beiträge** der Wert **An eine benutzerdefinierte Adresse** ausgewählt wurde.
Autoren bei Ablehnung von Beiträgen benach-	Gibt an, ob der Autor eines Beitrags benachrichtigt wird, wenn sein Beitrag durch die Moderatoren abgelehnt wurde. Wenn die Option aktiviert ist, erfassen Sie im Eingabefeld **Benachrichtigung an**

Eigenschaft	Beschreibung
richtigen	**Autor** einen Benachrichtigungstext.
Benachrichtigung an Autor	Benachrichtigung, die an Autoren gesendet wird, wenn ihr Beitrag abgelehnt wurde. Die maximale Textlänge ist 10.000 Zeichen. Benachrichtigungen werden nur gesendet, wenn die Option **Autoren bei Ablehnung von Beiträgen benachrichtigen** aktiviert ist.
Maximale Nachrichtengröße	Maximale Größe der Nachrichten, die an diese Gruppe gesendet werden können, in Bytes.
Google-Kommunikation zulassen	Gibt an, ob Google die Gruppenmanager kontaktieren darf.
Posten per Weboberfläche zulassen	Gibt an, ob Nutzer per Weboberfläche in der Gruppe posten dürfen. Wenn die Option deaktiviert ist, können die Nutzer nur GMail zur Kommunikation mit der Gruppe nutzen.
Im Namen der Gruppe posten	Gibt an, ob Gruppenmitglieder die E-Mail-Adresse der Gruppe nutzen dürfen, um Beiträge zu posten.
Nachrichten an die Gruppe archivieren	Gibt an, ob Nachrichten, die an die Gruppe gesendet wurden, archiviert werden sollen.
In globaler Adressliste anzeigen	Gibt an, ob die Gruppe in der globalen Adressliste angezeigt wird.
Gruppe im Verzeichnis aufführen	Gibt an, ob die Gruppe im Gruppenverzeichnis eingetragen werden soll.

Zusätzliche Aufgaben zur Verwaltung von G Suite Gruppen

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Aufgabe	Thema
Überblick über die G Suite Gruppe	Überblick über G Suite Gruppen auf Seite 139
Zusatzeigenschaften zuweisen	Zusatzeigenschaften an G Suite Gruppen zuweisen auf Seite 139
Gruppenmanager zuweisen	Gruppenmanager zuweisen auf Seite 140

Aufgabe	Thema
Gruppeneigentümer zuweisen	Gruppeneigentümer zuweisen
Benutzerkonten zuweisen	G Suite Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 104
Gruppen zuweisen	G Suite Gruppen an G Suite Gruppen zuweisen auf Seite 142
Kunde als Mitglied zuweisen	G Suite Kunden direkt an eine Gruppe zuweisen
Gruppen ausschließen	Wirksamkeit von G Suite Berechtigungszuweisungen auf Seite 106
Systemrollen zuweisen	G Suite Berechtigungen in Systemrollen aufnehmen auf Seite 101
Geschäftsrollen zuweisen	G Suite Berechtigungen an Geschäftsrollen zuweisen auf Seite 100
Organisationen zuweisen	G Suite Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 99
In IT Shop aufnehmen	G Suite Berechtigungen in den IT Shop aufnehmen auf Seite 102
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 44

Überblick über G Suite Gruppen

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

Um einen Überblick über eine Gruppe zu erhalten

1. Wählen Sie die Kategorie **G Suite | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die G Suite Gruppe**.

Zusatzeigenschaften an G Suite Gruppen zuweisen

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

Um Zusatzeigenschaften für eine Gruppe festzulegen

1. Wählen Sie im Manager die Kategorie **G Suite | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

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

Gruppenmanager zuweisen

Legen Sie die Gruppenmanager für eine Gruppe fest.

Um die Gruppenmanager für eine Gruppe festzulegen

1. Wählen Sie die Kategorie **G Suite | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppenmanager zuweisen**.
4. Wählen Sie in der Auswahlliste **Tabelle** die Tabelle **G Suite Benutzerkonten**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

HINWEIS: Standardmäßig können G Suite Kunden und Gruppen nicht als Gruppenmanager zugewiesen werden. In der Google Admin-Konsole sind diese Zuweisungen jedoch möglich. Wenn solche Zuweisungen im Zielsystem vorhanden sind, werden sie durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Bestehende Zuweisungen können im Manager angezeigt werden.

Um zu prüfen, ob Gruppen als Gruppenmanager an eine Gruppe zugewiesen sind

1. Wählen Sie die Kategorie **G Suite | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppenmanager zuweisen**.

4. Wählen Sie in der Auswahlliste **Tabelle** die Tabelle **G Suite Gruppen**.

   Im Bereich **Zuordnungen entfernen** werden alle zugewiesenen Gruppen angezeigt.

Um zu prüfen, ob der Kunde als Gruppenmanager an eine Gruppe zugewiesen ist

1. Wählen Sie die Kategorie **G Suite | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppenmanager zuweisen**.
4. Wählen Sie in der Auswahlliste **Tabelle** die Tabelle **G Suite Kunden**.

   Im Bereich **Zuordnungen entfernen** wird der zugewiesene Kunde angezeigt.

Im Manager können Kunden und Gruppen nicht als Gruppenmanager zugewiesen werden.

Gruppeneigentümer zuweisen

Legen Sie die Gruppeneigentümer für eine G Suite Gruppe fest.

Um Benutzerkonten als Gruppeneigentümer für eine Gruppe festzulegen

1. Wählen Sie die Kategorie **G Suite | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppeneigentümer zuweisen**.
4. Wählen Sie in der Auswahlliste **Tabelle** die Tabelle **G Suite Benutzerkonten**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

HINWEIS: Standardmäßig können G Suite Kunden und Gruppen nicht als Gruppeneigentümer zugewiesen werden. In der Google Admin-Konsole sind diese Zuweisungen jedoch möglich. Wenn solche Zuweisungen im Zielsystem vorhanden sind, werden sie durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Bestehende Zuweisungen können im Manager angezeigt werden.

Um zu prüfen, ob Gruppen als Gruppeneigentümer an eine Gruppe zugewiesen sind

1. Wählen Sie die Kategorie **G Suite | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppeneigentümer zuweisen**.
4. Wählen Sie in der Auswahlliste **Tabelle** die Tabelle **G Suite Gruppen**.

Im Bereich **Zuordnungen entfernen** werden alle zugewiesenen Gruppen angezeigt.

Um zu prüfen, ob der Kunde als Gruppeneigentümer an eine Gruppe zugewiesen ist

1. Wählen Sie die Kategorie **G Suite | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppeneigentümer zuweisen**.
4. Wählen Sie in der Auswahlliste **Tabelle** die Tabelle **G Suite Kunden**.

   Im Bereich **Zuordnungen entfernen** wird der zugewiesene Kunde angezeigt.

Im Manager können Kunden und Gruppen nicht als Gruppeneigentümer zugewiesen werden.

G Suite Gruppen an G Suite Gruppen zuweisen

G Suite Gruppen können selbst Mitglied anderer G Suite Gruppen sein. Damit können die Gruppen hierarchisch strukturiert werden.

Um Gruppen als Mitglieder an eine Gruppe zuzuweisen

1. Wählen Sie die Kategorie **G Suite | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Wählen Sie den Tabreiter **Hat Mitglieder**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die untergeordneten Gruppen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Um eine Gruppe als Mitglied in andere Gruppen aufzunehmen

1. Wählen Sie die Kategorie **G Suite | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Wählen Sie den Tabreiter **Ist Mitglied in**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die übergeordneten Gruppen zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Verwandte Themen

- G Suite Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 104

G Suite Gruppen löschen

Um eine Gruppe zu löschen

1. Wählen Sie im Manager die Kategorie **G Suite | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Klicken Sie .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Die Gruppe wird endgültig aus der One Identity Manager-Datenbank und der G Suite-Umgebung gelöscht.

G Suite Produkte und SKUs

Produkte und die zugehörigen Dienste sowie die zur Anmeldung benötigten Lizenzen werden im One Identity Manager als Produkte und SKUs (Stock-Keeping-Units) abgebildet. Um die Nutzer mit den benötigten Berechtigungen zur Anmeldung an der G Suite zu versorgen, weisen Sie die Produkt SKUs an die Benutzerkonten zu.

Stammdaten für G Suite Produkte und SKUs bearbeiten

Um die Stammdaten einer Produkt SKU zu bearbeiten

1. Wählen Sie im Manager die Kategorie **G Suite | Produkte und SKUs**.
2. Wählen Sie in der Ergebnisliste die Produkt SKU aus.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten der Produkt SKU.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für G Suite Produkte und SKUs auf Seite 144

Allgemeine Stammdaten für G Suite Produkte und SKUs

Für Produkte und SKUs bearbeiten Sie die folgenden Stammdaten.

Tabelle 42: Allgemeine Stammdaten einer Produkt SKU

Eigenschaft	Beschreibung
G Suite Kunde	Kunden-Umgebung, zu der die Produkt SKU gehört.
Produktname	Anzeigename des Produkts.
SKU Name	Anzeigename der SKU.
Leistungsposition	Angabe einer Leistungsposition, um die Produkt SKU über den IT Shop zu bestellen.
IT Shop	Angabe, ob die Produkt SKU über den IT Shop bestellbar ist. Die Produkt SKU kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Produkt SKU kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Produkt SKU ausschließlich über den IT Shop bestellbar ist. Die Produkt SKU kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Produkt SKU an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen an die Produkt SKU. Stellen Sie einen Wert zwischen **0** und **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung der Produkt SKU an Benutzerkonten. Produkt SKUs können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Produkt SKUs und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.

Verwandte Themen

- Vererbung von G Suite Berechtigungen anhand von Kategorien auf Seite 108
- G Suite Berechtigungen in den IT Shop aufnehmen auf Seite 102

Zusätzliche Aufgaben zur Verwaltung von G Suite Produkten und SKUs

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Aufgabe	Thema
Überblick über das G Suite Produkt und die SKU	Überblick über G Suite Produkte und SKUs auf Seite 145
Zusatzeigenschaften zuweisen	Zusatzeigenschaften an G Suite Produkte und SKUs zuweisen auf Seite 146
Benutzerkonten zuweisen	G Suite Benutzerkonten direkt an eine Berechtigung zuweisen auf Seite 104
Systemrollen zuweisen	G Suite Berechtigungen in Systemrollen aufnehmen auf Seite 101
Geschäftsrollen zuweisen	G Suite Berechtigungen an Geschäftsrollen zuweisen auf Seite 100
Organisationen zuweisen	G Suite Berechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 99
In IT Shop aufnehmen	G Suite Berechtigungen in den IT Shop aufnehmen auf Seite 102
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 44

Überblick über G Suite Produkte und SKUs

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

Um einen Überblick über eine Produkt SKU zu erhalten

1. Wählen Sie die Kategorie **G Suite | Produkte und SKUs**.
2. Wählen Sie in der Ergebnisliste die Produkt SKU.
3. Wählen Sie die Aufgabe **Überblick über das G Suite Produkt und die SKU**.

Zusatzeigenschaften an G Suite Produkte und SKUs zuweisen

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

Um Zusatzeigenschaften für eine Produkt SKU festzulegen

1. Wählen Sie im Manager die Kategorie **G Suite | Produkte und SKUs**.
2. Wählen Sie in der Ergebnisliste die Produkt SKU.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

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

G Suite Organisationen

Über Organisationen werden die Einstellungen für die Nutzer einer G Suite festgelegt. Pro Kunden-Umgebung gibt es genau eine übergeordnete Organisation. Unterhalb dieser können weitere Organisationen eingerichtet und so eine Organisationshierarchie aufgebaut werden. Untergeordnete Organisationen erben die Einstellungen der jeweils übergeordneten Organisation. Benutzerkonten sind genau einer Organisation zugeordnet.

G Suite Organisationen erstellen

Um eine Organisation zu erstellen

1. Wählen Sie im Manager die Kategorie **G Suite | Organisationen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Organisation.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für G Suite Organisationen auf Seite 147
- Stammdaten für G Suite Organisationen bearbeiten auf Seite 147

Stammdaten für G Suite Organisationen bearbeiten

Um die Stammdaten einer Organisation zu bearbeiten

1. Wählen Sie im Manager die Kategorie **G Suite | Organisationen**.
2. Wählen Sie in der Ergebnisliste die Organisation.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten der Organisation.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für G Suite Organisationen auf Seite 147
- G Suite Organisationen erstellen auf Seite 146

Allgemeine Stammdaten für G Suite Organisationen

Für Organisationen bearbeiten Sie die folgenden Stammdaten.

Tabelle 43: Allgemeine Stammdaten einer Organisation

Eigenschaft	Beschreibung
G Suite Kunde	Kunden-Umgebung, zu der die Organisation gehört.
ID der Organisation	Kennung der Organisation.
Name der Organisation	Anzeigename der Organisation.
Vollständiger Pfad	Vollständiger Pfad der Organisation.
Übergeordnete Organisation	Übergeordnete Organisation.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Zusätzliche Aufgaben zur Verwaltung von G Suite Organisationen

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Aufgabe	Thema
Überblick über die G Suite Organisation	Überblick über G Suite Organisationen auf Seite 148
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 44
Übergeordnete Organisation ändern	G Suite Organisationen verschieben auf Seite 148

Überblick über G Suite Organisationen

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

Um einen Überblick über eine Organisation zu erhalten

1. Wählen Sie die Kategorie **G Suite | Organisationen**.
2. Wählen Sie in der Ergebnisliste die Organisation.
3. Wählen Sie die Aufgabe **Überblick über die G Suite Organisation**.

G Suite Organisationen verschieben

Innerhalb einer Organisationshierarchie können untergeordnete Organisationen verschoben werden. Ordnen Sie dafür diesen Organisationen eine andere übergeordnete Organisation zu.

Um eine Organisation zu verschieben

1. Wählen Sie die Kategorie **G Suite | Organisationen**.
2. Wählen Sie in der Ergebnisliste die Organisation.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Übergeordnete Organisation ändern**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Wählen Sie in der Auswahlliste **Übergeordnete Organisation** die neuen Organisation.
7. Speichern Sie die Änderungen.

G Suite Organisationen löschen

Um eine Organisation zu löschen

1. Wählen Sie im Manager die Kategorie **G Suite | Organisationen**.
2. Wählen Sie in der Ergebnisliste die Organisation.
3. Klicken Sie .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Die Organisation wird endgültig aus der One Identity Manager-Datenbank und der G Suite-Umgebung gelöscht.

G Suite Domains

Als G Suite Domains werden im One Identity Manager die primäre Domain eines Kunden sowie weitere Internetdomains abgebildet. Domains werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können nicht bearbeitet werden. Über die Einzelobjektsynchronisation können Änderungen an den Objekteigenschaften einzelner Domains übernommen werden.

Um die Eigenschaften einer Domain anzuzeigen

1. Wählen Sie im Manager die Kategorie **G Suite | Domains**.
2. Wählen Sie in der Ergebnisliste die Domain.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Um einen Überblick über eine Domain zu erhalten

1. Wählen Sie im Manager die Kategorie **G Suite | Domains**.
2. Wählen Sie in der Ergebnisliste die Domain.
3. Wählen Sie die Aufgabe **Überblick über die G Suite Domain**.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 44

G Suite Domain-Aliasse

Über Domain-Aliasse erhalten die Nutzer einer primären Domain zusätzliche E-Mail-Adressen. Domain-Aliasse werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können nicht bearbeitet werden. Über die

Einzelobjektsynchronisation können Änderungen an den Objekteigenschaften einzelner Domain-Aliasse übernommen werden.

Um die Eigenschaften eines Domain-Alias anzuzeigen

1. Wählen Sie im Manager die Kategorie **G Suite | Domain-Aliasse**.
2. Wählen Sie in der Ergebnisliste den Domain-Alias.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Um einen Überblick über einen Domain-Alias zu erhalten

1. Wählen Sie im Manager die Kategorie **G Suite | Domain-Aliasse**.
2. Wählen Sie in der Ergebnisliste den Domain-Alias.
3. Wählen Sie die Aufgabe **Überblick über den G Suite Domain-Alias**.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 44

G Suite Admin-Rollen

Über Admin-Rollen werden den Nutzern administrative Berechtigungen in der G Suite gewährt. Benutzerdefinierte Admin-Rollen können im One Identity Manager angelegt werden. Damit die Nutzer die Berechtigungen erhalten, weisen Sie die Admin-Rollen an Benutzerkonten zu.

G Suite Admin-Rollen erstellen

Um eine Admin-Rolle zu erstellen

1. Wählen Sie im Manager die Kategorie **G Suite | Admin-Rollen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Admin-Rolle.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für G Suite Admin-Rollen auf Seite 151
- Stammdaten für G Suite Admin-Rollen bearbeiten auf Seite 151

Stammdaten für G Suite Admin-Rollen bearbeiten

Um die Stammdaten einer Admin-Rolle zu bearbeiten

1. Wählen Sie im Manager die Kategorie **G Suite | Admin-Rollen**.
2. Wählen Sie in der Ergebnisliste die Admin-Rolle.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten der Admin-Rolle.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für G Suite Admin-Rollen auf Seite 151
- G Suite Admin-Rollen erstellen auf Seite 150

Allgemeine Stammdaten für G Suite Admin-Rollen

Für Admin-Rollen bearbeiten Sie die folgenden Stammdaten.

Tabelle 44: Allgemeine Stammdaten einer Admin-Rolle

Eigenschaft	Beschreibung
G Suite Kunde	Kunden-Umgebung, zu der die Admin-Rolle gehört.
Kennung der Rolle	Eindeutige Kennung der Rolle. Für neue Admin-Rollen wird die Kennung im Zielsystem vergeben.
Name der Rolle	Anzeigename der Rolle.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Ist Super Admin	Gibt an, ob die Admin-Rolle eine Super Admin Rolle ist.
Ist System-rolle	Gibt an, ob die Admin-Rolle eine vordefinierte Admin-Rolle ist.

Zusätzliche Aufgaben zur Verwaltung von G Suite Admin-Rollen

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Aufgabe	Thema
Überblick über die G Suite Admin-Rolle	Überblick über G Suite Admin-Rollen auf Seite 152
Admin-Berechtigungen zuweisen	Admin-Berechtigungen an G Suite Admin-Rollen zuweisen auf Seite 152
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 44

Überblick über G Suite Admin-Rollen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Admin-Rolle.

Um einen Überblick über eine Admin-Rolle zu erhalten

1. Wählen Sie die Kategorie **G Suite | Admin-Rollen**.
2. Wählen Sie in der Ergebnisliste die Admin-Rolle.
3. Wählen Sie die Aufgabe **Überblick über die G Suite Admin-Rolle**.

Admin-Berechtigungen an G Suite Admin-Rollen zuweisen

Weisen Sie den benutzerdefinierten Admin-Rollen alle Berechtigungen zu, welche die Benutzerkonten über diese Admin-Rolle erhalten sollen.

Um Admin-Berechtigungen an eine benutzerdefinierte Admin-Rolle zuzuweisen

1. Wählen Sie im Manager die Kategorie **G Suite | Admin-Rollen**.
2. Wählen Sie in der Ergebnisliste die Admin-Rolle.
3. Wählen Sie die Aufgabe **Admin-Berechtigungen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Admin-Berechtigungen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Admin-Berechtigungen entfernen.

Um eine Zuweisung zu entfernen

- Wählen Sie die Admin-Berechtigung und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- G Suite Admin-Berechtigungen an Admin-Rollen zuweisen auf Seite 154

G Suite Admin-Rollen löschen

Benutzerdefinierte Admin-Rollen können im Manager gelöscht werden. Systemrollen dürfen nicht gelöscht werden.

Um eine benutzerdefinierte Admin-Rolle zu löschen

1. Wählen Sie im Manager die Kategorie **G Suite | Admin-Rollen**.
2. Wählen Sie in der Ergebnisliste die Admin-Rolle.
3. Klicken Sie .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Die Admin-Rolle wird endgültig aus der One Identity Manager-Datenbank und der G Suite-Umgebung gelöscht.

G Suite Admin-Berechtigungen

Admin-Berechtigungen bilden die administrativen Berechtigungen ab, die Benutzerkonten über die zugewiesenen Admin-Rollen erhalten. Admin-Berechtigungen werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können nicht bearbeitet werden. Über die Einzelobjektsynchronisation können Änderungen an den Objekteigenschaften einzelner Admin-Berechtigungen übernommen werden.

Stammdaten für G Suite Admin-Berechtigungen anzeigen

Um die Stammdaten einer Admin-Berechtigung anzuzeigen

1. Wählen Sie im Manager die Kategorie **G Suite | Admin-Berechtigungen**.
2. Wählen Sie in der Ergebnisliste die Admin-Berechtigung.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Verwandte Themen

- Überblick über G Suite Admin-Berechtigungen auf Seite 154

Zusätzliche Aufgaben zur Verwaltung von G Suite Admin-Berechtigungen

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Aufgabe	Thema
Überblick über die G Suite Admin-Berechtigung	Überblick über G Suite Admin-Berechtigungen auf Seite 154
Admin-Rollen zuweisen	G Suite Admin-Berechtigungen an Admin-Rollen zuweisen auf Seite 154
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 44

Überblick über G Suite Admin-Berechtigungen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Admin-Berechtigung.

Um einen Überblick über eine Admin-Berechtigung zu erhalten

1. Wählen Sie die Kategorie **G Suite | Admin-Berechtigungen**.
2. Wählen Sie in der Ergebnisliste die Admin-Berechtigung.
3. Wählen Sie die Aufgabe **Überblick über die G Suite Admin-Berechtigung**.

G Suite Admin-Berechtigungen an Admin-Rollen zuweisen

Weisen Sie eine Admin-Berechtigung an verschiedene benutzerdefinierte Admin-Rollen zu.

Um eine Admin-Berechtigungen an benutzerdefinierte Admin-Rollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **G Suite | Admin-Berechtigungen**.
2. Wählen Sie in der Ergebnisliste die Admin-Berechtigung.
3. Wählen Sie die Aufgabe **Admin-Rollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Admin-Rollen zu.

TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Admin-Rollen entfernen.

Um eine Zuweisung zu entfernen

- Wählen Sie die Admin-Rolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Admin-Berechtigungen an G Suite Admin-Rollen zuweisen auf Seite 152

G Suite Admin-Rollen-Zuordnungen

Administrative Berechtigungen können auf einzelne Organisation eingeschränkt werden. Dafür werden die Admin-Rollen an Organisationen zugeordnet. Benutzerkonten, denen solch eine Admin-Rolle zugewiesen ist, können die damit verbundenen administrativen Berechtigungen nur in der zugeordneten Organisation anwenden.

G Suite Admin-Rollen-Zuordnungen erstellen

Um eine Organisation an eine Admin-Rolle zuzuordnen

1. Wählen Sie im Manager die Kategorie **G Suite | Admin-Rollen-Zuordnungen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Zuordnung.
    - Wählen Sie aus der Auswahlliste **Admin-Rolle** die Admin-Rolle.
    - Wählen Sie aus der Auswahlliste **G Suite Organisation** die Organisation.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Benutzerkonten an G Suite Admin-Rollen-Zuordnungen zuweisen auf Seite 156

Zusätzliche Aufgaben zur Verwaltung von G Suite Admin-Rollen-Zuordnungen

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Aufgabe	Thema
Überblick über die G Suite Admin-Rollen-Zuordnung	Überblick über G Suite Admin-Rollen-Zuordnungen auf Seite 156
Benutzerkonten zuweisen	Benutzerkonten an G Suite Admin-Rollen-Zuordnungen zuweisen auf Seite 156
Objekt synchronisieren	Einzelobjekte synchronisieren auf Seite 44

Überblick über G Suite Admin-Rollen-Zuordnungen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Admin-Rollen-Zuordnung.

Um einen Überblick über eine Admin-Rollen-Zuordnung zu erhalten

1. Wählen Sie die Kategorie **G Suite | Admin-Rollen-Zuordnungen**.
2. Wählen Sie in der Ergebnisliste die Admin-Rollen-Zuordnung.
3. Wählen Sie die Aufgabe **Überblick über die G Suite Admin-Rollen-Zuordnung**.

Benutzerkonten an G Suite Admin-Rollen-Zuordnungen zuweisen

Weisen Sie den Admin-Rollen-Zuordnungen alle Benutzerkonten zu, die administrative Berechtigungen für die Organisation erhalten sollen.

Um Benutzerkonten an eine Admin-Rollen-Zuordnung zuzuweisen

1. Wählen Sie im Manager die Kategorie **G Suite | Admin-Rollen-Zuordnungen**.
2. Wählen Sie in der Ergebnisliste die Admin-Rollen-Zuordnung.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

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

   Um eine Zuweisung zu entfernen

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

G Suite Admin-Rollen-Zuordnungen löschen

Um eine Admin-Rollen-Zuordnung zu löschen

1. Wählen Sie im Manager die Kategorie **G Suite | Admin-Rollen-Zuordnungen**.
2. Wählen Sie in der Ergebnisliste die Admin-Rollen-Zuordnung.
3. Klicken Sie .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Die Admin-Rollen-Zuordnung wird endgültig aus der One Identity Manager-Datenbank und der G Suite-Umgebung gelöscht.

Berichte über G Suite Objekte

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

Tabelle 45: Berichte für das Zielsystem

Bericht	Beschreibung
Übersicht aller Zuweisungen (Kunde)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die in der ausgewählten Kunden-Umgebung mindestens ein Benutzerkonto besitzen.
Übersicht aller Zuweisungen (Gruppe)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, welche die ausgewählte Gruppe besitzen.
Übersicht aller Zuweisungen (Produkt und SKU)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, welche die ausgewählte Produkt SKU besitzen.
G Suite Benutzerkonten- und Gruppenverteilung	Der Bericht enthält eine Zusammenfassung zur Benutzerkonten- und Berechtigungsverteilung aller Kunden-Umgebungen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager| Übersichten Zielsysteme**.
Ungenutzte Benutzerkonten anzeigen	Der Bericht enthält alle Benutzerkonten der ausgewählten Kunden-Umgebung, die in den letzten Monaten nicht verwendet wurden. Der Bericht enthält die Mitgliedschaften in Gruppen und Produkt SKUs und die Risikoeinschätzung. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager| Analyse Datenqualität**.
Abweichende System-	Der Bericht enthält alle Berechtigungen der ausgewählten

Bericht	Beschreibung
berechtigungen anzeigen	Kunden-Umgebung, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager| Analyse Datenqualität**.
Benutzerkonten mit einer überdurchschnittlichen Anzahl an Systemberechtigungen anzeigen	Der Bericht enthält alle Benutzerkonten der ausgewählten Kunden-Umgebung, die eine überdurchschnittliche Anzahl an zugewiesenen Gruppen und Produkt SKUs besitzen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager| Analyse Datenqualität**.
Unverbundene Benutzerkonten anzeigen	Der Bericht enthält alle unverbundenen Benutzerkonten der ausgewählten Kunden-Umgebung einschließlich ihrer zugeordneten Gruppen und Produkt SKUs. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager| Analyse Datenqualität**.
Datenqualität der G Suite Benutzerkonten	Der Bericht enthält verschiedenen Auswertungen zur Datenqualität der Benutzerkonten aller Kunden-Umgebungen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager | Analyse Datenqualität**.

7

Behandeln von G Suite Objekten im Web Portal

Der One Identity Manager bietet seinen Benutzern die Möglichkeit, verschiedene Aufgaben unkompliziert über ein Web Portal zu erledigen. Das Web Portal unterstützt die Administration einer G Suite bei folgenden Aufgaben:

- Managen von Benutzerkonten und Personen

  Mit der Zuweisung einer Kontendefinition an ein IT Shop Regal kann die Kontendefinition von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Person, beispielsweise einen Manager, wird das Benutzerkonto angelegt.

- Managen von Berechtigungszuweisungen

  Mit der Zuweisung einer G Suite Berechtigung an ein IT Shop Regal kann die Berechtigung von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Person wird die Berechtigung zugewiesen.

  Manager und Administratoren von Organisationen können im Web Portal G Suite Berechtigungen an die Abteilungen, Kostenstellen oder Standorte zuweisen, für die sie verantwortlich sind. Die Berechtigungen werden an alle Personen vererbt, die Mitglied dieser Abteilungen, Kostenstellen oder Standorte sind.

  Wenn das Geschäftsrollenmodul vorhanden ist, können Manager und Administratoren von Geschäftsrollen im Web Portal G Suite Berechtigungen an die Geschäftsrollen zuweisen, für die sie verantwortlich sind. Die Berechtigungen werden an alle Personen vererbt, die Mitglied dieser Geschäftsrollen sind.

  Wenn das Systemrollenmodul vorhanden ist, können Verantwortliche von Systemrollen im Web Portal G Suite Berechtigungen an die Systemrollen zuweisen. Die Berechtigungen werden an alle Personen vererbt, denen diese Systemrollen zugewiesen sind.

- Attestierung

  Wenn das Modul Attestierung vorhanden ist, kann die Richtigkeit der Eigenschaften von Zielsystemobjekten und von Berechtigungszuweisungen regelmäßig oder auf Anfrage bescheinigt werden. Dafür werden im Manager Attestierungsrichtlinien

konfiguriert. Die Attestierer nutzen das Web Portal, um Attestierungsvorgänge zu entscheiden.

- Governance Administration

  Wenn das Modul Complianceregeln vorhanden ist, können Regeln definiert werden, die unzulässige Berechtigungszuweisungen identifizieren und deren Risiken bewerten. Die Regeln werden regelmäßig und bei Änderungen an den Objekten im One Identity Manager überprüft. Complianceregeln werden im Manager definiert. Verantwortliche Personen nutzen das Web Portal, um Regelverletzungen zu überprüfen, aufzulösen und Ausnahmegenehmigungen zu erteilen.

  Wenn das Modul Unternehmensrichtlinien vorhanden ist, können Unternehmensrichtlinien für die im One Identity Manager abgebildeten Zielsystemobjekte definiert und deren Risiken bewertet werden. Unternehmensrichtlinien werden im Manager definiert. Verantwortliche Personen nutzen das Web Portal, um Richtlinienverletzungen zu überprüfen und Ausnahmegenehmigungen zu erteilen.

- Risikobewertung

  Über den Risikoindex von G Suite Berechtigungen kann das Risiko von Berechtigungszuweisungen für das Unternehmen bewertet werden. Dafür stellt der One Identity Manager Standard-Berechnungsvorschriften bereit. Im Web Portal können die Berechnungsvorschriften modifiziert werden.

- Berichte und Statistiken

  Das Web Portal stellt verschiedene Berichte und Statistiken über die Personen, Benutzerkonten, deren Berechtigungen und Risiken bereit.

Ausführliche Informationen zu den genannten Themen finden Sie unter Zuweisen von G Suite Berechtigungen an Benutzerkonten im One Identity Manager auf Seite 97 und in folgenden Handbüchern:

- One Identity Manager Anwenderhandbuch für das Web Portal
- One Identity Manager Administrationshandbuch für Attestierungen
- One Identity Manager Administrationshandbuch für Complianceregeln
- One Identity Manager Administrationshandbuch für Unternehmensrichtlinien
- One Identity Manager Administrationshandbuch für Risikobewertungen

8

Basisdaten für die Verwaltung einer G Suite

Für die Verwaltung einer G Suite im One Identity Manager sind folgende Basisdaten relevant.

- Kontendefinitionen

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

  Weitere Informationen finden Sie unter Kontendefinitionen für G Suite Benutzerkonten auf Seite 51.

- Kennwortrichtlinien

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

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

  Weitere Informationen finden Sie unter Kennwortrichtlinien für G Suite Benutzerkonten auf Seite 83.

- Zielsystemtypen

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

  Weitere Informationen finden Sie unter Ausstehende Objekte nachbearbeiten auf Seite 45.

- Server

  Für die Verarbeitung der G Suite-spezifischen Prozesse im One Identity Manager muss der Synchronisationsserver mit seinen Serverfunktionen bekannt sein.

  Weitere Informationen finden Sie unter Jobserver für G Suite-spezifische Prozessverarbeitung auf Seite 162.

- Zielsystemverantwortliche

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

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

  Weitere Informationen finden Sie unter Zielsystemverantwortliche für Kunden-Umgebungen auf Seite 167.

Jobserver für G Suite-spezifische Prozessverarbeitung

Für die Verarbeitung der G Suite-spezifischen Prozesse im One Identity Manager muss der Synchronisationsserver mit seinen Serverfunktionen bekannt sein. Um die Funktion eines Servers zu definieren, haben Sie mehrere Möglichkeiten:

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

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

Verwandte Themen

- Systemanforderungen für den G Suite Synchronisationsservers auf Seite 18

G Suite Jobserver bearbeiten

Um einen Jobserver und seine Funktionen zu bearbeiten

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Jobserver auf Seite 163
- Festlegen der Serverfunktionen auf Seite 166

Allgemeine Stammdaten für Jobserver

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

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

Tabelle 46: Eigenschaften eines Jobservers

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS Syntax. Beispiel: `<Name des Servers>.<Vollqualifizierter Domänenname>`
Zielsystem	Zielsystem des Computerkontos.
Sprachkultur	Sprache des Servers.
Server ist Cluster	Angabe, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. HINWEIS: Die Eigenschaften **Server ist Cluster** und **Server gehört zu Cluster** schließen einander aus.

Eigenschaft	Bedeutung
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.
IP-Adresse (IPv4)	Internet Protokoll Version 4 (IPv4)-Adresse des Servers.
Kopierverfahren (Quellserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Quelle einer Kopieraktion ist. Derzeit werden nur Kopierverfahren über die Programme Robocopy und rsync unterstützt. Wird kein Verfahren angegeben, ermittelt der One Identity Manager Service zur Laufzeit das Betriebssystem des Servers, auf dem die Kopieraktion ausgeführt wird. Die Replikation erfolgt dann zwischen Servern mit einem Windows Betriebssystem mit dem Programm Robocopy und zwischen Servern mit einem Linux Betriebssystem mit dem Programm rsync. Unterscheiden sich die Betriebssysteme des Quellservers und des Zielservers, so ist für eine erfolgreiche Replikation die Angabe der zulässigen Kopierverfahren zwingend erforderlich. Es wird das Kopierverfahren eingesetzt, das beide Server unterstützen.
Kopierverfahren (Zielserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Ziel einer Kopieraktion ist.
Codierung	Codierung des Zeichensatzes mit der Dateien auf dem Server geschrieben werden.
Übergeordneter Jobserver	Bezeichnung des übergeordneten Jobservers.
Ausführender Server	Bezeichnung des ausführenden Servers. Eingetragen wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden. Diese Angabe wird bei der automatischen Aktualisierung des One Identity Manager Service ausgewertet. Verarbeitet ein Server mehrere Queues, wird mit der Auslieferung von Prozessschritten solange gewartet, bis alle Queues, die auf demselben Server abgearbeitet werden, die automatische Aktualisierung abgeschlossen haben.
Queue	Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Serverbetriebssystem	Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt.

Eigenschaft	Bedeutung
	Zulässig sind die Werte **Win32**, **Windows**, **Linux** und **Unix**. Ist die Angabe leer, wird **Win32** angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen.
One Identity Manager Service installiert	Angabe, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur `QBM_PJobQueueLoad` aktiviert, sobald die Queue das erste Mal angefragt wird. Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.
Stopp One Identity Manager Service	Angabe, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten. Den Dienst können Sie mit entsprechenden administrativen Rechten im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*.
Kein automatisches Softwareupdate	Angabe, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.
Softwareupdate läuft	Angabe, ob gerade eine Softwareaktualisierung ausgeführt wird.
Letzter Abrufzeitpunkt	Zeitpunkt der letzten Prozessabholung.
Letzte Timeout Prüfung	Zeitpunkt der letzten Prüfung für geladene Prozessschritte, deren Auslieferung den Wert im Konfigurationsparameter **Common | Jobservice | LoadedJobsTimeOut** überschreitet.
Serverfunktion	Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

Verwandte Themen

- Festlegen der Serverfunktionen auf Seite 166

Festlegen der Serverfunktionen

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

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

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

Tabelle 47: Zulässige Serverfunktionen

Serverfunktion	Anmerkungen
Aktualisierungsserver	Der Server führt die automatische Softwareaktualisierung aller anderen Server aus. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Der Server kann SQL Aufträge ausführen. Bei der initialen Schemainstallation wird der Server, auf dem die One Identity Manager-Datenbank installiert ist, mit dieser Serverfunktion gekennzeichnet.
SQL Ausführungsserver	Der Server kann SQL Aufträge ausführen. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Für eine Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.
CSV Skriptserver	Der Server kann CSV-Dateien per Prozesskomponente `ScriptComponent` verarbeiten.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
SMTP Host	Server, auf dem durch den One Identity Manager Service E-Mail Benachrichtigungen verschickt werden. Voraussetzung zum Versenden von Mails durch den One Identity Manager Service ist ein konfigurierter SMTP Host.
Standard Berichtserver	Server, auf dem die Berichte generiert werden.
G Suite Konnektor	Server, auf dem der G Suite Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem G Suite aus.

Verwandte Themen

- Allgemeine Stammdaten für Jobserver auf Seite 163

Zielsystemverantwortliche für Kunden-Umgebungen

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

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

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

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

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

   Zielsystemverantwortliche der Standardanwendungsrolle sind berechtigt alle Kunden-Umgebungen im One Identity Manager zu bearbeiten.
3. Zielsystemverantwortliche können innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche berechtigen und bei Bedarf weitere untergeordnete Anwendungsrollen erstellen und einzelnen Kunden-Umgebungen zuweisen.

Tabelle 48: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | G Suite** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen. • Bearbeiten Kennwortrichtlinien für das Zielsystem.

Benutzer	Aufgaben
	• Bereiten Berechtigungen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Um initial Personen als Zielsystemadministrator festzulegen

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

Um initial Personen in die Standardanwendungsrolle für Zielsystemverantwortliche aufzunehmen

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

Um als Zielsystemverantwortlicher weitere Personen als Zielsystemverantwortliche zu berechtigen

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

Um Zielsystemverantwortliche für einzelne Kunden-Umgebungen festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **G Suite | Kunden-Umgebungen**.
3. Wählen Sie in der Ergebnisliste die Kunden-Umgebung.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Zielsystemverantwortliche** die Anwendungsrolle.

   - ODER -

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

   a. Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Zielsysteme | G Suite** zu.

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

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer G Suite auf Seite 10
- Allgemeine Stammdaten für G Suite Kunden auf Seite 113

Beheben von Fehlern beim Anbinden einer G Suite-Umgebung

Neu angelegte G Suite Benutzerkonten werden als ausstehend markiert

Wenn kurz nach der Provisionierung neuer Benutzerkonten in die G Suite eine Synchronisation in die One Identity Manager-Datenbank ausgeführt wird, kann es vorkommen, dass diese Benutzerkonten im One Identity Manager als ausstehend markiert werden (oder gelöscht werden, je nach Konfiguration der Synchronisation). Der Fehler tritt nur auf, wenn im Synchronisationsprojekt für das Zielsystem ein Scope definiert wurde.

Wahrscheinliche Ursache

Das Anlegen eines neuen Benutzerkontos in der G Suite dauert etwa 24 Stunden. Wenn innerhalb dieser 24 Stunden eine Synchronisation in die One Identity Manager-Datenbank gestartet wird, kann der beschriebene Fehler auftreten.

Lösung

Damit der Fehler nicht auftritt

- Vermeiden Sie die Definition eines Scopes für das Zielsystem.

Wenn ein Scope benötigt wird

1. Konfigurieren Sie die Synchronisation von Benutzerkonten so, dass Objekte, die im One Identity Manager nicht vorhanden sind, als ausstehend markiert werden.
2. Wenn der Fehler auftritt, führen Sie einen Zielsystemabgleich durch.

   Weitere Informationen finden Sie unter Ausstehende Objekte nachbearbeiten auf Seite 45.

   a. Wählen Sie die Objekte, die fälschlicherweise als ausstehend markiert wurden.

   b. Wenden Sie die Methode **Zurücksetzen** an.

Die Markierung **Ausstehend** wird entfernt. Bei der nächsten Synchronisation, die nach den 24 Stunden ausgeführt wird, sollte der Fehler nicht mehr auftreten.

Ausführliche Informationen zur Definition eines Scopes und zur Festlegung von Verarbeitungsmethoden für Synchronisationsschritte finden Sie im One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation.

Anhang A

Konfigurationsparameter für die Verwaltung einer G Suite

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

Tabelle 49: Konfigurationsparameter für die Synchronisation einer G Suite

Konfigurationsparameter	Bedeutung bei Aktivierung
TargetSystem | GoogleApps	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung des Zielsystems G Suite. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.
TargetSystem | GoogleApps | Accounts	Parameter zur Konfiguration der Angaben zu G Suite Benutzerkonten.
TargetSystem | GoogleApps | Accounts | InitialRandomPassword	Der Konfigurationsparameter legt fest, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in der zugewiesenen Kennwortrichtlinie definiert sind.
TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo	Angabe, welche Person die E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Geschäftsrolle, Verantwortlicher der Person oder `XUserInserted`). Ist kein Empfänger ermittelbar, dann wird die E-Mail an die im Konfigurationsparameter **TargetSystem | GoogleApps | DefaultAddress** hinterlegte Adresse versandt.
TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den Anmeldeinformationen zum Benutzerkonto zu versorgen. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto** verwendet.

Konfigurationsparameter	Bedeutung bei Aktivierung
TargetSystem | GoogleApps | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den Informationen zum initialen Kennwort zu versorgen. Es wird die Mailvorlage **Person - Initiales Kennwort für neues Benutzerkonto** verwendet.
TargetSystem | GoogleApps | Accounts | MailTemplateDefaultValues	Der Konfigurationsparameter enthält die Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto mit Standardwerten** verwendet.
TargetSystem | GoogleApps | Accounts | PrivilegedAccount	Der Konfigurationsparameter erlaubt die Konfiguration der Einstellungen für privilegierte Benutzerkonten.
TargetSystem | GoogleApps | Accounts | TransferJPegPhoto	Der Konfigurationsparameter legt fest, ob bei Änderung des Bildes in den Stammdaten der Person dieses an bestehende G Suite Benutzerkonten publiziert wird. Das Bild ist nicht Bestandteil der normalen Synchronisation, es wird nur bei Änderung der Personenstammdaten publiziert.
TargetSystem | GoogleApps | DefaultAddress	Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem | GoogleApps | MaxFullsyncDuration	Der Konfigurationsparameter enthält die maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.
TargetSystem | GoogleApps | PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem | GoogleApps | PersonAutoDisabledAccounts	Der Konfigurationsparameter legt fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem | GoogleApps | PersonAutoFullsync	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt

Konfigurationsparameter	Bedeutung bei Aktivierung
	oder aktualisiert werden.
TargetSystem | GoogleApps | PersonExcludeList	Der Konfigurationsparameter enthält eine Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird.

Anhang B

Standardprojektvorlage für eine G Suite

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

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

Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 50: Abbildung der G Suite Schematypen auf Tabellen im One Identity Manager Schema

Schematyp in der G Suite	Tabelle im One Identity Manager Schema
AdminPrivilege	GAPPrivilege
AdminRole	GAPAdminRole
AdminRoleAssignment	GAPOrgAdminRole
Customer	GAPCustomer
Domain	GAPDomain
DomainAlias	GAPDomainAlias
Group	GAPGroup
OrgUnit	GAPOrgUnit
ProductAndSku	GAPPaSku
User	GAPUser
UserAddress	GAPUserAddress

Schematyp in der G Suite	Tabelle im One Identity Manager Schema
UserEmail	GAPUserEmail
UserExternalId	GAPUserExternalId
UserIm	GAPUserIM
UserOrganization	GAPUserOrganization
UserPhone	GAPUserPhone
UserRelation	GAPUserRelation
UserWebsite	GAPUserWebSite

Anhang C

API-Bereiche für das Dienstkonto

In der Google Admin-Konsole muss die Client-ID des Dienstkontos auf verschiedene API-Bereiche autorisiert werden.

Für den Lese- und Schreibzugriff:

```
https://www.googleapis.com/auth/admin.directory.customer,
https://www.googleapis.com/auth/admin.directory.device.chromeos,
https://www.googleapis.com/auth/admin.directory.device.mobile,
https://www.googleapis.com/auth/admin.directory.device.mobile.action,
https://www.googleapis.com/auth/admin.directory.domain,
https://www.googleapis.com/auth/admin.directory.group,
https://www.googleapis.com/auth/admin.directory.group.member,
https://www.googleapis.com/auth/admin.directory.notifications,
https://www.googleapis.com/auth/admin.directory.orgunit,
https://www.googleapis.com/auth/admin.directory.resource.calendar,
https://www.googleapis.com/auth/admin.directory.rolemanagement,
https://www.googleapis.com/auth/admin.directory.user,
https://www.googleapis.com/auth/admin.directory.user.alias,
https://www.googleapis.com/auth/admin.directory.user.security,
https://www.googleapis.com/auth/admin.directory.userschema,
https://www.googleapis.com/auth/apps.groups.settings,
https://www.googleapis.com/auth/admin.datatransfer,
https://www.googleapis.com/auth/apps.licensing
```

Für den Nur-Lese-Zugriff:

```
https://www.googleapis.com/auth/admin.directory.customer.readonly,
https://www.googleapis.com/auth/admin.directory.device.chromeos.readonly,
https://www.googleapis.com/auth/admin.directory.device.mobile.readonly,
https://www.googleapis.com/auth/admin.directory.domain.readonly,
https://www.googleapis.com/auth/admin.directory.group.readonly,
https://www.googleapis.com/auth/admin.directory.group.member.readonly,
https://www.googleapis.com/auth/admin.directory.orgunit.readonly,
https://www.googleapis.com/auth/admin.directory.resource.calendar.readonly,
https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly,
https://www.googleapis.com/auth/admin.directory.user.readonly,
```

```
https://www.googleapis.com/auth/admin.directory.user.alias.readonly,
https://www.googleapis.com/auth/admin.directory.userschema.readonly,
https://www.googleapis.com/auth/apps.groups.settings,
https://www.googleapis.com/auth/admin.datatransfer.readonly,
https://www.googleapis.com/auth/apps.licensing
```

Anhang D

Verarbeitung von Systemobjekten einer G Suite

Folgende Tabelle beschreibt die zulässigen Verarbeitungsmethoden für die Schematypen der G Suite und benennt notwendige Einschränkungen bei der Verarbeitung der Systemobjekte.

Tabelle 51: Zulässige Verarbeitungsmethoden für Schematypen

Schematyp	Lesen	Einfügen	Löschen	Aktualisieren
G Suite Kunde (`Customer`)	ja	nein	nein	ja
Domain (`Domain`)	ja	nein	nein	nein
Domain-Alias (`DomainAlias`)	ja	nein	nein	nein
Organisation (`OrgUnit`)	ja	ja	ja	ja
Benutzerkonto (`User`)	ja	ja	ja	ja
Gruppe (`Group`)	ja	ja	ja	ja
Produkt und SKU (`ProductAndSku`)	ja	nein	nein	ja
Benutzerkonto: Adresse (`UserAddress`)	ja	ja	ja	ja
Benutzerkonto: E-Mail-Adresse (`UserEmail`)	ja	ja	ja	ja
Benutzerkonto: externe ID (`UserExternalId`)	ja	ja	ja	ja
Benutzerkonto: Instant Messenger (`UserIm`)	ja	ja	ja	ja
Benutzerkonto: Nutzerdetails (`UserOrganization`)	ja	ja	ja	ja
Benutzerkonto: Telefonnummer (`UserPhone`)	ja	ja	ja	ja
Benutzerkonto: Beziehung (`UserRelation`)	ja	ja	ja	ja

Schematyp	Lesen	Einfügen	Löschen	Aktualisieren
Benutzerkonto: Website (`UserWebsite`)	ja	ja	ja	ja
Admin-Rolle (`AdminRole`)	ja	ja	ja	ja
Admin-Berechtigung (`AdminPrivilege`)	ja	nein	nein	nein
Admin-Rollen-Zuordnung (`AdminRoleAssignment`)	ja	ja	ja	ja

Anhang E

Besonderheiten bei der Zuweisung von G Suite Gruppen

Im One Identity Manager können Berechtigungen direkt oder indirekt an Benutzerkonten zugewiesen werden. Die Art der Zuweisung wird an den Zuweisungstabellen in der Spalte `XOrigin` gekennzeichnet. In den Zuweisungstabellen `GAPUserInPaSku` und `GAPUserInGroup` kann `XOrigin` die Standardwerte **1** bis **15** (Bit 0 bis 3) annehmen.

Über die Zuweisung einer G Suite Gruppe an einen G Suite Kunden können alle Benutzerkonten des Kunden Mitglied dieser Gruppe werden. Bei der Vererbungsberechnung wird für alle Benutzerkonten des Kunden ein Eintrag in der Tabelle `GAPUserInGroup` erstellt. Die Herkunft dieser Zuweisungen wird in `GAPUserInGroup.XOrigin` mit dem Wert **16** (Bit 4) gekennzeichnet.

Tabelle 52: Herkunft von Berechtigungszuweisungen

Zuweisungstabelle	Art der Zuweisung	Herkunft (Spalte `XOrigin`)
GAPUserInPaSku GAPUserInGroup	direkt	1
	indirekt	2
	dynamisch	4
	Zuweisungsbestellung	8
GAPUserInGroup	über Kunden	16

Ausführliche Informationen zur Berechnung von Zuweisungen im One Identity Manager finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- Zuweisen von G Suite Berechtigungen an Benutzerkonten im One Identity Manager auf Seite 97

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

Index

C

D

E

G

I

J

K

L

M

N

O

P

R

S

T

V

W

X

Z