One Identity Manager 8.0.1

# Administrationshandbuch für die Anbindung einer G Suite-Umgebung

**Legende**

**WARNUNG: Das Symbol WARNUNG weist auf mögliche Personen- oder Sachschäden oder Schaden mit Todesfolge hin.**

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

WICHTIG, HINWEIS, TIPP, MOBIL, or VIDEO: Ein Informationssymbol weist auf Begleitinformationen hin.

One Identity Manager Administrationshandbuch für die Anbindung einer G Suite-Umgebung
Aktualisiert - April 2018
Version - 8.0.1

# Inhalt

# Verwalten einer G Suite

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.

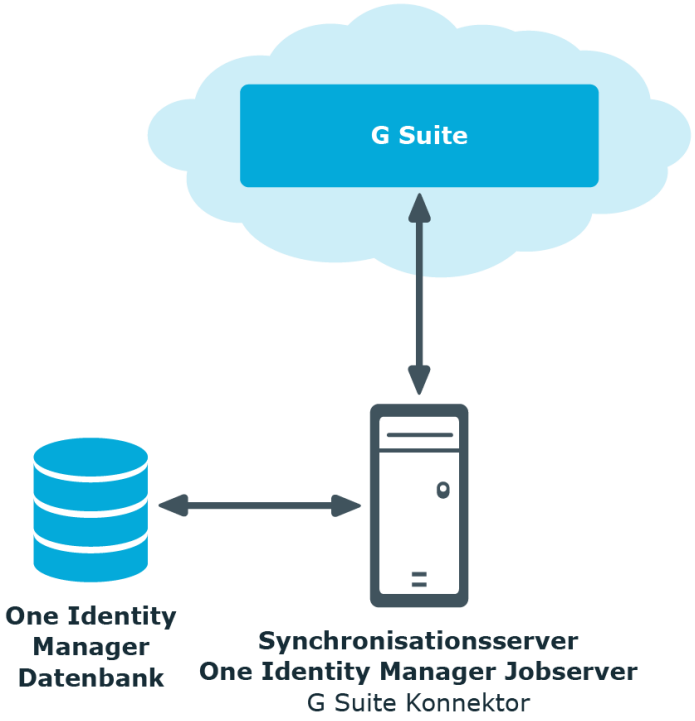
Im One Identity Manager werden die Personen eines Unternehmens mit den benötigten Benutzerkonten versorgt. Dabei können Sie unterschiedliche Mechanismen für die Verbindung der Personen mit ihren Benutzerkonten nutzen. Ebenso können Sie die Benutzerkonten getrennt von Personen verwalten und somit administrative 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.<br>Benutzer mit dieser Anwendungsrolle:<br>• Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen.<br>• Legen die Zielsystemverantwortlichen fest.<br>• Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein.<br>• Legen sich fest, welche Anwendungsrollen für Zielsys- |

| Benutzer | Aufgaben |
| --- | --- |
| | temverantwortliche sich widersprechen.<br>• Berechtigen weitere Personen als Zielsystemadministratoren.<br>• Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme. |
| Zielsystemverantwortliche | Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme \| G Suite** oder einer untergeordneten Anwendungsrolle zugewiesen sein.<br>Benutzer mit dieser Anwendungsrolle:<br>• Übernehmen die administrativen Aufgaben für das Zielsystem.<br>• Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen.<br>• Bearbeiten Kennwortrichtlinien für das Zielsystem.<br>• Bereiten Systemberechtigungen zur Aufnahme in den IT Shop vor.<br>• Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.<br>• Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation.<br>• 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.<br>• Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen.<br>• Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter.<br>• Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse.<br>• Erstellen und konfigurieren bei Bedarf Zeitpläne.<br>• Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien. |

# 2

# Einrichten der Synchronisation mit 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.

***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 10
- Einrichten des Synchronisationsservers auf Seite 13
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer G Suite auf Seite 16
- Deaktivieren der Synchronisation auf Seite 37
- Anpassen einer Synchronisationskonfiguration auf Seite 24
- Anhang: Konfigurationsparameter für die Verwaltung einer G Suite auf Seite 81

- Anhang: Standardprojektvorlage für eine G Suite auf Seite 84
- Anhang: Verarbeitung von Systemobjekten auf Seite 86

# 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 die G Suite | 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.<br>• Das Google Cloud Platform Projekt benötigt Zugriff auf folgende APIs:<br>Admin SDK<br>Enterprise License Manager API<br>Groups Settings API<br>• Zur Authentifizierung wird ein Dienstkonto mit der zugehörigen JSON-Schlüsseldatei und domainübergreifender G Suite-Delegation benötigt.<br>• In der Google Admin-Konsole muss der API-Zugriff aktiviert sein.<br>• In der Google Admin-Konsole muss die Client-ID des Dienstkontos auf folgende API-Bereiche autorisiert werden:<br>`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,` |

| Benutzer | Berechtigungen |
|---|---|
| | `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`<br><br>Weitere Informationen finden Sie unter Einrichten der erforderlichen Berechtigungen für den Zugriff auf die G Suite auf Seite 12. |
| Benutzerkonto des One Identity Manager Service | Das Benutzerkonto für den One Identity Manager Service benötigt die Rechte, um die Operationen auf Dateiebene durchzuführen (Rechtevergabe, Verzeichnisse und Dateien anlegen und bearbeiten).<br><br>Das Benutzerkonto muss der Gruppe "Domänen-Benutzer" (Domain Users) angehören.<br><br>Das Benutzerkonto benötigt das erweiterte Benutzerrecht "Anmelden als Dienst" (Log on as a service).<br><br>Das Benutzerkonto benötigt Rechte für den internen Webservice.<br><br>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:<br><br>`netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"`<br><br>Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis.<br><br>In der Standardinstallation wird der One Identity Manager installiert unter:<br><br>• `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen)<br>• `%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. |

# 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 G Suite 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 die G Suite auf Seite 10.
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 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 ab Version 8.1
- Windows Server

  Unterstützt werden die Versionen:

  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
- Microsoft .NET Framework Version 4.5.2 oder höher

  HINWEIS: Microsoft .NET Framework Version 4.6 wird nicht unterstützt.

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.
- One Identity Manager Service, G Suite Konnektor
  - Installieren Sie die One Identity Manager Komponenten mit dem Installationsassistenten.
    1. Wählen Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen**.
    2. Wählen Sie die Maschinenrolle **Server | Jobserver | 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. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein.

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

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

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

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

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

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

      - ODER -

      Um einen neuen Jobserver zur erstellen, klicken Sie **Hinzufügen**.
   b. Bearbeiten Sie folgende Informationen für den Jobserver.

**Tabelle 4: Eigenschaften eines Jobservers**

| Eigenschaft | Beschreibung |
|---|---|
| Server | Bezeichnung des Jobservers. |
| Queue | Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen. |
| Vollständiger Servername | Vollständiger Servername gemäß DNS Syntax.<br>Beispiel:<br>`<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** legen Sie fest, welche Rolle der Jobserver im One Identity Manager übernimmt. Abhängig von der gewählten Maschinenrolle werden die Installationspakete ermittelt, die auf dem Jobserver installiert werden.
   - G Suite
5. Auf der Seite **Serverfunktionen** legen Sie die Funktion des Servers in der One Identity Manager-Umgebung fest. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

   Die Serverfunktionen sind abhängig von den gewählten Maschinenrollen bereits ausgewählt. Sie können die Serverfunktionen hier weiter einschränken.
   - G Suite Konnektor
6. Auf der Seite **Dienstkonfiguration** 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.
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.

**Tabelle 5: Installationsinformationen**

| Eingabe | Beschreibung |
|---|---|
| Computer | Server, auf dem der Dienst installiert und gestartet wird.<br>***Um einen Server auszuwählen***<br>• Erfassen Sie den Servernamen.<br>-ODER-<br>• Wählen Sie einen Eintrag in der Liste. |
| Dienstkonto | Angaben zum Benutzerkonto des One Identity Manager Service.<br>***Um ein Benutzerkonto für den One Identity Manager*** |

| Eingabe | Beschreibung |
|---|---|
| | ***Service zu erfassen***<br>• Aktivieren Sie die Option **Lokales Systemkonto**.<br>Damit wird der One Identity Manager Service unter dem Konto "NT AUTHORITY\SYSTEM" gestartet.<br>- ODER-<br>• Erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung. |
| Installationskonto | Angaben zum administrativen Benutzerkonto für die Installation des Dienstes.<br>***Um ein administratives Benutzerkonto für die Installation zu erfassen***<br>• Aktivieren Sie die Option **Erweitert**.<br>• Aktivieren Sie die Option **Angemeldeter Benutzer**.<br>Es wird das Benutzerkonto des aktuell angemeldeten Benutzers verwendet.<br>- ODER-<br>• Geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein. |

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

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

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

    HINWEIS: Der Dienst wird 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.

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

**Tabelle 6: 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.<br>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 10. |
| 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.<br>Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem G Suite Konnektor installiert sein.<br>**Tabelle 7: Zusätzliche Eigenschaften für den Jobserver**<br>Eigenschaft: Serverfunktion — Wert: G Suite Konnektor<br>Eigenschaft: Maschinenrolle — Wert: Server/Jobserver/G Suite<br>Weitere Informationen finden Sie unter Einrichten des Synchronisationsservers auf Seite 13. |
| Verbindungsdaten zur One Identity Manager Datenbank | SQL Server:<br>• Datenbankserver |

| Angaben | Erläuterungen |
| --- | --- |
| | • Datenbank<br>• Datenbankbenutzer und Kennwort<br>• Angabe, ob integrierte Windows Authentifizierung verwendet wird.<br>Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows Authentifizierung unterstützt.<br>Oracle:<br>• Angabe, ob der Zugriff direkt oder über Oracle Client erfolgt<br>Die erforderlichen Verbindungsdaten sind abhängig von der Einstellung dieser Option.<br>• Datenbankserver<br>• Port der Oracle Instanz<br>• Service Name<br>• Oracle Datenbankbenutzer und Kennwort<br>• Datenquelle (TNS Alias Name aus der `TNSNames.ora`) |
| 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.<br>Der Remoteverbindungsserver und die Arbeitsstation müssen in der selben Active Directory Domäne stehen.<br>Konfiguration des Remoteverbindungsservers:<br>• One Identity Manager Service ist gestartet<br>• `RemoteConnectPlugin` ist installiert<br>• G Suite Konnektor ist installiert<br>Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des |

| Angaben | Erläuterungen |
| --- | --- |
| | Jobservers benötigt.<br><br>TIPP: Der Remoteverbindungsserver benötigt dieselbe Konfiguration (bezüglich der installierten Software) wie der Synchronisationsserver. Nutzen Sie den Synchronisationsserver gleichzeitig als Remoteverbindungsserver, indem Sie lediglich das `RemoteConnectPlugin` zusätzlich installieren.<br><br>Ausführliche Informationen zum Herstellen einer Remoteverbindung finden Sie im One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation. |

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

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

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

### *Um ein initiales Synchronisationsprojekt für eine G Suite einzurichten*

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

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

2. Wählen Sie den Eintrag **Zielsystemtyp G Suite**. 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 8: 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.<br>• Ziehen Sie die Schlüsseldatei per Drag and Drop in das Eingabefeld, um sie zu laden.<br>- ODER -<br>• 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.

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 9: 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.<br>Der Synchronisationsworkflow zeigt folgende Besonderheiten:<br>• Die Synchronisationsrichtung ist "In den One Identity Manager".<br>• 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.<br>Der Provisionierungsworkflow zeigt folgende Besonderheiten:<br>• Die Synchronisationsrichtung ist "In das Zielsystem".<br>• In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung "In das Zielsystem" definiert.<br>• 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.

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

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

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

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

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

### *Um den Inhalt des Synchronisationsprotokolls zu konfigurieren*

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

    HINWEIS: Einige Inhalte erzeugen besonders viele Protokolldaten!

    Das Synchronisationsprotokoll soll nur die für Fehleranalysen und weitere Auswertungen notwendigen Daten enthalten.

6. Klicken Sie **OK**.

### *Um regelmäßige Synchronisationen auszuführen*

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

***Um die initiale Synchronisation manuell zu starten***

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

HINWEIS: Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Personen erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für 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***

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie der Kunden-Umgebung eine Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand "Linked" (verbunden) die Kontendefinition und den Automatisierungsgrad zu.
    a. Wählen Sie die Kategorie **G Suite | Benutzerkonten | Verbunden aber nicht konfiguriert | <Kunden-Umgebung>**.
    b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.

### Verwandte Themen

- Einrichten des Synchronisationsservers auf Seite 13
- Benutzer und Berechtigungen für die Synchronisation mit einer G Suite auf Seite 10
- Synchronisationsergebnisse anzeigen auf Seite 23
- Anpassen einer Synchronisationskonfiguration auf Seite 24
- Erweiterte Einstellungen der Zielsystemverbindung auf Seite 28
- Anhang: Standardprojektvorlage für eine G Suite auf Seite 84

# Synchronisationsergebnisse anzeigen

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

***Um das Protokoll einer Synchronisation anzuzeigen***

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

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

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

***Um das Protokoll einer Provisionierung anzuzeigen***

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

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

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

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

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt. Den Aufbewahrungszeitraum legen Sie über den Konfigurationsparameter "DPR\Journal\LifeTime" und seine untergeordneten Konfigurationsparameter fest.

***Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen***

- Aktivieren Sie im Designer den Konfigurationsparameter "Common\Journal\LifeTime" und tragen Sie die maximale Aufbewahrungszeit für die Einträge im Systemprotokoll ein. Mit den untergeordneten Konfigurationsparametern legen Sie die Aufbewahrungszeit je Meldungstyp fest.
- Bei großen Datenmengen können Sie zur Performance-Optimierung die Menge der zu löschenden Objekte pro Operation und Verarbeitungslauf des DBQueue Prozessor festlegen. Verwenden Sie dazu die Konfigurationsparameter "Common\Journal\Delete\BulkCount" und "Common\Journal\Delete\TotalCount".
- Konfigurieren und aktivieren Sie im Designer den Zeitplan "Journal löschen".

# Anpassen einer Synchronisationskonfiguration

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.

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 Daten zu synchronisieren, für die keine Schematypen im Konnektorschema angelegt sind, legen Sie eigene Schematypen an.

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.
- 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. Gruppieren Sie die Startkonfigurationen mit gleichem Startverhalten.

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

### Detaillierte Informationen zum Thema

- Synchronisation in die G Suite konfigurieren auf Seite 26
- Synchronisation verschiedener Kunden-Umgebungen konfigurieren auf Seite 26
- Schema aktualisieren auf Seite 27
- Erweiterte Einstellungen der Zielsystemverbindung auf Seite 28

# 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 26

# Synchronisation verschiedener Kunden-Umgebungen konfigurieren

Für alle Kunden-Umgebungen, die mit dem selben Synchronisationsprojekt synchronisiert werden sollen, müssen die folgenden Voraussetzungen gewährleistet sein.

***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.

***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 26

# 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. Wählen Sie die Kategorie **Konfiguration | Zielsystem**.

   - ODER -

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

   Die Schemadaten werden neu geladen.

***Um ein Mapping zu bearbeiten***

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

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

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

# Erweiterte Einstellungen der Zielsystemverbindung

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 31.

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

   Der Systemverbindungsassistent liefert zusätzliche Erläuterungen zu den Einstellungen. Die Standardwerte werden jedoch überschrieben. Sie können nicht zurückgesetzt werden.

   Weitere Informationen finden Sie unter Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 32.

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 10: Erweiterte Einstellungen der Zielsystemverbindung**

| Eigenschaft | Beschreibung |
|---|---|
| Lokalen Cache verwenden | Angabe, ob der lokale Cache des G Suite Konnektors genutzt werden soll.<br>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.<br>Die Option ist standardmäßig aktiviert. Für Fehleranalysen kann sie deaktiviert werden.<br>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.<br>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. |

| Eigenschaft | Beschreibung |
| --- | --- |
| 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. |
| Produkte und SKUs XML | Produkt-IDs und Stock-Keeping-Unit-IDs als XML-Datei.<br>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.<br>Beispiel:<br>`<products>`<br>`<product name="G Suite" id="Google-Apps">`<br>`<sku id="Google-Apps-Unlimited" name="G Suite Business"/>`<br>`<sku id="Google-Apps-For-Business" name="G Suite Basic" />`<br>`<sku id="Google-Apps-Lite" name="G Suite Lite"/>`<br>`<sku id="Google-Apps-For-Postini" name="Google Apps Message Security"/>`<br>`</product>`<br>`<product name="Google Drive storage" id="Google-Drive-storage">`<br>`<sku id="Google-Drive-storage-20GB" name="Google Drive storage 20 GB"/>`<br>`<sku id="Google-Drive-storage-50GB" name="Google Drive storage 50 GB"/>`<br>`<...>`<br>`<sku id="Google-Drive-storage-16TB" name="Google Drive storage 16 TB"/>`<br>`</product>`<br>`<...>`<br>`</products>` |

# 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**.
4. Wählen Sie einen der folgenden Parameter und klicken Sie **Umwandeln**.

   **Tabelle 11: Variablen für die erweiterten Einstellungen der Systemverbindung**

   | Parameter | Beschreibung |
   |---|---|
   | 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. |
   | 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. |
   | Cache | Angabe, ob der lokale Cache des G Suite Konnektors genutzt werden soll. |

   Weitere Informationen finden Sie unter Erweiterte Einstellungen der Zielsystemverbindung auf Seite 28.
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 Eigenschaften der Zielsystemverbindung können auch mit dem Systemverbindungsassistenten geändert werden. Dabei werden die Werte, die Sie hier setzen in das Standardvariablenset übernommen. Die ursprünglichen Standardwerte können folglich nicht wiederhergestellt werden.

***Um die erweiterten Einstellungen mit dem Systemverbindungsassistenten zu bearbeiten***

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

   Der Systemverbindungsassistent wird gestartet.
4. Auf der Startseite des Systemverbindungsassistenten aktivieren Sie **Erweiterte Einstellungen anzeigen**.

5. Auf der Seite **Erweiterte Einstellungen** passen Sie die Eigenschaften Ihren Erfordernissen an.

   Weitere Informationen finden Sie unter Erweiterte Einstellungen der Zielsystemverbindung auf Seite 28.
6. Speichern Sie die Änderungen.

# Beschleunigung der Synchronisation durch Revisionsfilterung

Die Synchronisation mit einer G Suite unterstützt keine Revisionsfilterung.

# Nachbehandlung ausstehender Objekte

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

Objekte, die als ausstehend gekennzeichnet wurden,

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

Führen Sie dafür einen Zielsystemabgleich durch.

***Um ausstehende Objekte nachzubearbeiten***

1. Wählen Sie die Kategorie **G Suite | Zielsystemabgleich: G Suite**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp G Suite als Synchronisationstabellen zugewiesen sind.
2. Wählen Sie in der Navigationsansicht die Tabelle, für die sie ausstehende Objekte nachbearbeiten möchten.

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

   TIPP:

   ***Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen***

   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 12: 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.<br>Indirekte Mitgliedschaften können nicht gelöscht werden. |
|  | Publizieren | Das Objekt wird im Zielsystem eingefügt. Die Markierung "Ausstehend" wird für das Objekt entfernt.<br>Die Methode löst das Ereignis "HandleOutstanding" aus. Dadurch wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt.<br>Voraussetzungen:<br>• Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen.<br>• Der Zielsystemkonnektor kann schreibend auf das Zielsystem zugreifen. |
|  | Zurücksetzen | Die Markierung "Ausstehend" wird für das Objekt entfernt. |

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

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

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

***Um die Massenverarbeitung zu deaktivieren***

- Deaktivieren Sie in der Formularsymbolleiste .

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

***Um Tabellen in den Zielsystemabgleich aufzunehmen***

1. Wählen Sie 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.

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

# Provisionierung von Mitgliedschaften konfigurieren

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

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

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

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

***Um die Einzelprovisionierung von Mitgliedschaften zu ermöglichen***

1. Starten Sie den Manager.
2. Wählen Sie die Kategorie **G Suite | Basisdaten zur Konfiguration | Zielsystemtypen**.
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 **Änderungen zusammenführen**.
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.

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

# Unterstützung bei der Analyse von Synchronisationsproblemen

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

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

***Um den Synchronisationsanalysebericht zu erstellen***

1. Wählen Sie das Menü **Hilfe | Synchronisationsanalysebericht erstellen** und beantworten Sie die Sicherheitsabfrage mit **Ja**.

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

# Deaktivieren der Synchronisation

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

***Um regelmäßige Synchronisationen zu verhindern***

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

  Synchronisationen können nun nur noch manuell gestartet werden.

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

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

***Um das geladene Synchronisationsprojekt zu deaktivieren***

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

## Verwandte Themen

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer G Suite auf Seite 16

# 3

# Basisdaten für die Verwaltung einer G Suite

Für die Verwaltung einer G Suite im One Identity Manager sind folgende Basisdaten relevant.

- Konfigurationsparameter

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

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

  Weitere Informationen finden Sie unter Anhang: Konfigurationsparameter für die Verwaltung einer G Suite auf Seite 81.

- Kontendefinitionen

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

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

- 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 eine 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 auf Seite 58.

- Initiales Kennwort für neue Benutzerkonten

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

  Weitere Informationen finden Sie unter Initiales Kennwort für neue G Suite Benutzerkonten auf Seite 68.

- E-Mail-Benachrichtigungen über die Anmeldeinformationen

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

  Weitere Informationen finden Sie unter E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 69.

- Zielsystemtypen

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

  Weitere Informationen finden Sie unter Nachbehandlung ausstehender Objekte auf Seite 33.

- 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 Bearbeiten eines Servers auf Seite 71.

- 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 auf Seite 76.

# Einrichten von Kontendefinitionen

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

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

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

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

- Erstellen einer Kontendefinition auf Seite 40
- Erstellen der Automatisierungsgrade auf Seite 43
- Erstellen einer Abbildungsvorschrift für IT Betriebsdaten auf Seite 46
- Erfassen der IT Betriebsdaten auf Seite 47
- Zuweisen der Kontendefinition an Personen auf Seite 50
- Zuweisen der Kontendefinition an ein Zielsystem auf Seite 56

# Erstellen einer Kontendefinition

***Um eine Kontendefinition zu erstellen***

1. Wählen Sie die Kategorie **G Suite | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Kontendefinition.
4. Speichern Sie die Änderungen.

### Detaillierte Informationen zum Thema

- Stammdaten einer Kontendefinition auf Seite 41

# Stammdaten einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

**Tabelle 13: 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.<br>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.<br>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 |

| Eigenschaft | Beschreibung |
| --- | --- |
| | Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig. |
| Automatische Zuweisung zu Personen | Angabe, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Beim Speichern wird die Kontendefinition an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine Person neu angelegt wird, erhält sie ebenfalls automatisch diese Kontendefinition.<br>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!<br>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.<br>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.<br>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.<br>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.<br>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.<br>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.<br>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.<br>Option aktiviert: Die Zuweisung der Kontendefinition bleibt |

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

# Erstellen der Automatisierungsgrade

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

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

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

- Unmanaged

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

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

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

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

Legen Sie für jeden Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf

deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll. Ausführliche Informationen zu Automatisierungsgraden finden Sie im One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

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

***Um Automatisierungsgrade an eine Kontendefinition zuzuweisen***

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

   - ODER -

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

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

***Um einen Automatisierungsgrad zu bearbeiten***

1. Wählen Sie die Kategorie **G Suite | Basisdaten zur Konfiguration | Kontendefinitionen | Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Automatisierungsgrades.
4. Speichern Sie die Änderungen.

## Verwandte Themen

- Stammdaten eines Automatisierungsgrades auf Seite 45

# Stammdaten eines Automatisierungsgrades

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

**Tabelle 14: 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:<br>**Niemals**: Die Daten werden nicht aktualisiert.<br>**Immer**: Die Daten werden immer aktualisiert<br>**Nur initial**: Die Daten werden nur initial ermittelt. |
| Gruppen bei zeitweiliger Deaktivierung beibehalten | Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen. |
| Benutzerkonten bei zeitweiliger Deaktivierung sperren | Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen gesperrt werden sollen. |
| Gruppen bei dauerhafter Deaktivierung beibehalten | Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen. |
| Benutzerkonten bei dauerhafter Deaktivierung sperren | Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen gesperrt werden sollen. |
| Gruppen bei verzögertem Löschen beibehalten | Angabe, ob die Benutzerkonten zum Löschen markierter Personen ihre Gruppenmitgliedschaften behalten sollen. |
| Benutzerkonten bei verzögertem Löschen sperren | Angabe, ob die Benutzerkonten zum Löschen markierter Personen gesperrt werden sollen. |
| Gruppen bei Sicherheitsgefährdung beibehalten | Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen ihre Gruppenmitgliedschaften behalten sollen. |
| Benutzerkonten bei Sicherheitsgefährdung sperren | Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen gesperrt werden sollen. |

| Eigenschaft | Beschreibung |
| --- | --- |
| Gruppen bei deaktiviertem Benutzerkonto beibehalten | Angabe, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen. |

# Erstellen einer Abbildungsvorschrift für IT Betriebsdaten

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

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

- 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 die Kategorie **G Suite | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **IT Betriebsdaten Mapping bearbeiten** und erfassen Sie folgende Daten.

**Tabelle 15: Abbildungsvorschrift für IT Betriebsdaten**

| Eigenschaft | Beschreibung |
| --- | --- |
| Spalte | Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. |
| Quelle | Angabe, welche Rolle verwendet wird, um die Eigenschaften für das Benutzerkonto zu ermitteln. Zur Auswahl stehen:<br>• Primäre Abteilung<br>• Primärer Standort<br>• Primäre Kostenstelle |

| Eigenschaft | Beschreibung |
|---|---|
| | • Primäre Geschäftsrolle<br>HINWEIS: Verwenden Sie die primäre Geschäftsrolle nur, wenn das Geschäftsrollenmodul vorhanden ist.<br>• keine Angabe<br>Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option **Immer Standardwert verwenden** setzen. |
| Standardwert | Standardwert der Eigenschaft für das Benutzerkonto einer Person, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann. |
| Immer Standardwert verwenden | Angabe, ob die Eigenschaft des Benutzerkontos immer mit dem Standardwert besetzt wird. Es erfolgt keine dynamische Ermittlung der IT Betriebsdaten aus einer Rolle. |
| Benachrichtigung bei Verwendung des Standards | Angabe, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage "Person - Erstellung neues Benutzerkontos mit Standardwerten" verwendet. Um die Mailvorlage zu ändern, passen Sie den Konfigurationsparameter "TargetSystem\GoogleApps\Accounts\MailTemplateDefaultValues" an. |

4. Speichern Sie die Änderungen.

### Verwandte Themen

- Erfassen der IT Betriebsdaten auf Seite 47

# Erfassen der IT Betriebsdaten

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

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

Beispiel:

In der Regel erhält jede Person der Abteilung A ein Standardbenutzerkonto 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 in der Kategorie **Organisationen** bzw. **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten** und erfassen Sie folgende Daten.

**Tabelle 16: IT Betriebsdaten**

| Eigenschaft | Beschreibung |
|---|---|
| Organisation/Geschäftsrolle | Abteilung, Kostenstelle, Standort oder Geschäftsrolle, für die die IT Betriebsdaten gelten sollen. |
| Wirksam für | Anwendungsbereich der IT Betriebsdaten. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden.<br>***Um den Anwendungsbereich festzulegen***<br>a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.<br>b. Wählen Sie unter **Tabelle** die Tabelle, die das Zielsystem abbildet oder für eine Konten-definition die Tabelle `TSBAccountDef`.<br>c. Wählen Sie unter **Wirksam für** das konkrete Zielsystem oder die konkrete Kontendefinition.<br>d. Klicken Sie **OK**. |
| Spalte | Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird.<br>In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche |

| Eigenschaft | Beschreibung |
|---|---|
| | Informationen dazu finden Sie im One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul. |
| Wert | Konkreter Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll. |

3. Speichern Sie die Änderungen.

### Verwandte Themen

- Erstellen einer Abbildungsvorschrift für IT Betriebsdaten auf Seite 46

# Ändern der IT Betriebsdaten

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

***Voraussetzungen***

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

  - ODER -

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

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

***Um die Bildungsregeln auszuführen***

1. Wählen Sie die Kategorie **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 Kontendefinition an Personen

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

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

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

## Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

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

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

### Detaillierte Informationen zum Thema

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 51
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 52
- Kontendefinition an alle Personen zuweisen auf Seite 52
- Kontendefinition direkt an Personen zuweisen auf Seite 53
- Kontendefinition an Systemrollen zuweisen auf Seite 53
- Kontendefinition in den IT Shop aufnehmen auf Seite 54
- Zuweisen der Kontendefinition an ein Zielsystem auf Seite 56

# Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen

***Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen***

1. Wählen Sie 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.

   - ODER -

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

### Verwandte Themen

- Kontendefinition an Geschäftsrollen zuweisen auf Seite 52
- Kontendefinition an alle Personen zuweisen auf Seite 52
- Kontendefinition direkt an Personen zuweisen auf Seite 53
- Kontendefinition an Systemrollen zuweisen auf Seite 53
- Kontendefinition in den IT Shop aufnehmen auf Seite 54

# Kontendefinition an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

***Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen***

1. Wählen Sie 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.

   - ODER -

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

## Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 51
- Kontendefinition an alle Personen zuweisen auf Seite 52
- Kontendefinition direkt an Personen zuweisen auf Seite 53
- Kontendefinition an Systemrollen zuweisen auf Seite 53
- Kontendefinition in den IT Shop aufnehmen auf Seite 54

# Kontendefinition an alle Personen zuweisen

***Um eine Kontendefinition an alle Personen zuzuweisen***

1. Wählen Sie 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.

### Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 51
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 52
- Kontendefinition direkt an Personen zuweisen auf Seite 53
- Kontendefinition an Systemrollen zuweisen auf Seite 53
- Kontendefinition in den IT Shop aufnehmen auf Seite 54

## Kontendefinition direkt an Personen zuweisen

***Um eine Kontendefinition direkt an Personen zuzuweisen***

1. Wählen Sie 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.

   - ODER -

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

### Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 51
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 52
- Kontendefinition an alle Personen zuweisen auf Seite 52
- Kontendefinition an Systemrollen zuweisen auf Seite 53
- Kontendefinition in den IT Shop aufnehmen auf Seite 54

## Kontendefinition an Systemrollen zuweisen

Installierte Module: Systemrollenmodul

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

***Um Kontendefinitionen in eine Systemrolle aufzunehmen***

1. Wählen Sie 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.

   - ODER -

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

### Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 51
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 52
- Kontendefinition an alle Personen zuweisen auf Seite 52
- Kontendefinition direkt an Personen zuweisen auf Seite 53
- Kontendefinition in den IT Shop aufnehmen auf Seite 54

## Kontendefinition in den IT Shop aufnehmen

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

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

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 die Kategorie **G Suite | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

***Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen***

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

   - ODER -

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

***Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen***

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

   - ODER -

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

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

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

### Verwandte Themen

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

# Zuweisen der Kontendefinition an ein Zielsystem

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

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

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

***Um die Kontendefinition an ein Zielsystem zuzuweisen***

1. Wählen Sie in der Kategorie **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

- Zuweisen der Kontendefinition an Personen auf Seite 50

# Löschen einer Kontendefinition

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

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

***Um eine Kontendefinition zu löschen***

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Personen.
    a. Wählen Sie die Kategorie **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 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 Standorte.
    a. Wählen Sie 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 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 dazu finden Sie im One Identity Manager Administrationshandbuch für IT Shop.
6. Entfernen Sie die Zuordnung der Kontendefinition als vorausgesetzte Kontendefinition einer anderen Kontendefinition. Solange die Kontendefinition Voraussetzung einer anderen Kontendefinition ist, kann sie nicht gelöscht werden.

Prüfen Sie alle Kontendefinitionen.

a. Wählen Sie die Kategorie **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 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 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.

# 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 eine 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 59
- Bearbeiten von Kennwortrichtlinien auf Seite 60
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 62
- Ausschlussliste für Kennwörter auf Seite 65
- Prüfen eines Kennwortes auf Seite 65

- Generieren eines Kennwortes testen auf Seite 66
- Zuweisen einer Kennwortrichtlinie auf Seite 66

# 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" verwendet. 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`).

Die Kennwortrichtlinie "One Identity Manager Kennwortrichtlinie" ist zusätzlich als Standardrichtlinie gekennzeichnet und wird angewendet, wenn keine andere Kennwortrichtlinie ermittelt werden kann.

### 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`).

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

### Kennwortrichtlinien für Zielsysteme

Für jedes Zielsystem wird eine vordefinierte Kennwortrichtlinie bereitgestellt, die Sie auf die Kennwortspalten der Benutzerkonten anwenden können.

WICHTIG: Wenn Sie nicht mit zielsystemspezifischen Kennwortrichtlinien arbeiten, wirkt die Standardrichtlinie. Stellen Sie in diesem Fall sicher, dass die Kennwortrichtlinie "One Identity Manager Kennwortrichtlinie" 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.

# Bearbeiten von Kennwortrichtlinien

***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 und wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Kennwortrichtlinie.
4. Speichern Sie die Änderungen.

## Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Kennwortrichtlinie auf Seite 60
- Richtlinieneinstellungen auf Seite 61
- Zeichenklassen für Kennwörter auf Seite 62
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 62

# Allgemeine Stammdaten einer Kennwortrichtlinie

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

**Tabelle 17: 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. |

| Eigenschaft | Bedeutung |
| --- | --- |
| | HINWEIS: Die Kennwortrichtlinie "One Identity Manager Kennwortrichtlinie" ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn keine andere Kennwortrichtlinie ermittelt werden kann. |

# Richtlinieneinstellungen

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

**Tabelle 18: Richtlinieneinstellungen**

| Eigenschaft | Bedeutung |
| --- | --- |
| Initiales Kennwort | Initiales Kennwort für neu erzeugte Benutzerkonten. Wird beim Anlegen im Benutzerkonto selbst kein Kennwort angegeben oder ein Zufallskennwort generiert, dann wird das initiale Kennwort benutzt. |
| 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. |
| Max. Fehlanmeldungen | Anzahl der maximalen Fehlanmeldungen. Legen Sie die Anzahl der ungültigen Kennworteingaben fest. Hat ein Benutzer diese Anzahl erreicht, wird das Benutzerkonto gesperrt. |
| 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 5 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. |

| Eigenschaft | Bedeutung |
| --- | --- |
| Namensbestandteile unzulässig | Angabe, ob Namensbestandteile im Kennwort zulässig sind. |

# Zeichenklassen für Kennwörter

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

**Tabelle 19: 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. |
| Unzulässige Sonderzeichen | Liste unzulässiger 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. |

# 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 63
- Skript zum Generieren eines Kennwortes auf Seite 64

# 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 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 64

# 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 die unzulässige Zeichen "?" und "!" in Zufallskennwörtern.

```
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 63

# Ausschlussliste für Kennwörter

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.

# Prüfen eines Kennwortes

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 eines Kennwortes 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.

# Zuweisen einer Kennwortrichtlinie

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.

WICHTIG: Wenn Sie nicht mit zielsystemspezifischen Kennwortrichtlinien arbeiten, wirkt die Standardrichtlinie. Stellen Sie in diesem Fall sicher, dass die Kennwortrichtlinie "One Identity Manager Kennwortrichtlinie" 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 20: Zuweisen einer Kennwortrichtlinie**

| Eigenschaft | Beschreibung |
|---|---|
| Anwenden auf | Anwendungsbereich der Kennwortrichtlinie.<br>***Um den Anwendungsbereich festzulegen***<br>a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.<br>b. Wählen Sie unter **Tabelle** die Tabelle, die die Kennwortspalte enthält.<br>c. Wählen Sie unter **Anwenden auf** das konkrete Zielsystem.<br>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.

# Initiales Kennwort für neue G Suite Benutzerkonten

**Tabelle 21: Konfigurationsparameter für die Bildung eines initialen Kennwortes für Benutzerkonten**

| Konfigurationsparameter | Bedeutung |
|---|---|
| QER\Person\UseCentralPassword | Der Konfigurationsparameter legt fest, ob das zentrale Kennwort einer Person in den Benutzerkonten verwendet werden soll. Das zentrale Kennwort der Person wird automatisch auf die Benutzerkonten der Person in allen erlaubten Zielsystemen abgebildet. Ausgenommen sind privilegierte Benutzerkonten; diese werden nicht aktualisiert. |
| QER\Person\UseCentralPassword\ PermanentStore | Der Konfigurationsparameter steuert die Aufbewahrungszeit der zentralen Kennworte. Ist der Parameter aktiviert, wird das zentrale Kennwort der Person dauerhaft gespeichert. Ist der Parameter nicht aktiviert, wird das zentrale Kennwort nur zum Publizieren an bestehende zielsystemspezifische Benutzerkonten benutzt und anschließend in der One Identity Manager-Datenbank gelöscht. |
| 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. |

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

- Verwenden Sie das zentrale Kennwort der Person. Das zentrale Kennwort der zugeordneten Person wird auf das Kennwort des Benutzerkontos abgebildet.
  - Aktivieren Sie im Designer den Konfigurationsparameter "QER\Person\UseCentralPassword".

    Ist der Konfigurationsparameter "QER\Person\UseCentralPassword" aktiviert, wird das zentrale Kennwort der Person automatisch auf die Benutzerkonten einer Person in den einzelnen Zielsystemen abgebildet. Ausgenommen sind privilegierte Benutzerkonten; diese werden nicht aktualisiert.
  - Aktivieren Sie im Designer den Konfigurationsparameter "QER\Person\UseCentralPassword\PermanentStore" und legen Sie fest, ob das

zentrale Kennwort der Personen dauerhaft oder nur bis zum Publizieren in die Zielsysteme in der One Identity Manager-Datenbank gespeichert wird.

Bei der Bildung des zentralen Kennwortes wird die Kennwortrichtlinie "Kennwortrichtlinie für zentrales Kennwort von Personen" angewendet.

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

- Erstellen Sie Benutzerkonten manuell und tragen Sie in den Stammdaten der Benutzerkonten ein Kennwort ein.
- Legen Sie ein initiales Kennwort fest, welches beim Erstellen von Benutzerkonten automatisch verwendet wird.
  - Verwenden Sie zielsystemspezifische Kennwortrichtlinien und tragen Sie in den Kennwortrichtlinien ein initiales 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.

### Verwandte Themen

- Kennwortrichtlinien auf Seite 58
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 69

# E-Mail-Benachrichtigungen über Anmeldeinformationen

**Tabelle 22: Konfigurationsparameter für Benachrichtigungen über Aktionen im Zielsystem**

| Konfigurationsparameter | Bedeutung |
|---|---|
| TargetSys-tem\GoogleApps\DefaultAddress | Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsys-tem. |
| TargetSystem\GoogleApps\Accounts\ | Der Konfigurationsparameter enthält die |

| Konfigurationsparameter | Bedeutung |
|---|---|
| InitialRandomPassword\SendTo | Person, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Geschäftsrolle, Verantwortlicher der Person oder `XUserInserted`). Ist kein Empfänger ermittelbar, dann wird an die im Konfigurationsparameter "TargetSystem\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 initialen Anmeldeinformationen (Name des Benutzerkontos) zu versorgen. Es wird die Mailvorlage "Person - Erstellung neues Benutzerkonto" verwendet. |
| TargetSystem\GoogleApps\Accounts\ InitialRandomPassword\SendTo\ MailTemplatePassword | Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den initialen Anmeldeinformationen (initiales Kennwort) zu versorgen. Es wird die Mailvorlage "Person - Initiales Kennwort für neues Benutzerkonto" verwendet. |

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

***Um Benachrichtigungen über Anmeldeinformationen zu nutzen***

1. Stellen Sie sicher, dass das E-Mail-Benachrichtungssystem im One Identity Manager konfiguriert ist. Ausführliche Informationen finden Sie im One Identity Manager Konfigurationshandbuch.
2. Aktivieren Sie im Designer den Konfigurationsparameter "Common\MailNotification\DefaultSender" und geben Sie die Absenderadresse an, mit der die E-Mail Benachrichtigungen verschickt werden.
3. Stellen Sie sicher, dass alle Personen eine Standard-E-Mail-Adresse besitzen. An diese E-Mail Adresse werden die Benachrichtigungen versendet. Ausführliche

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

4. Stellen Sie sicher, dass für alle Personen eine Sprachkultur ermittelt werden kann. Nur so erhalten die Personen die E-Mail Benachrichtigungen in ihrer Sprache. Ausführliche Informationen finden Sie im 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.
3. Aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\GoogleApps\Accounts\InitialRandomPassword\SendTo\MailTemplate AccountName".

   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\MailTemplate Password".

   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.

# Bearbeiten eines Servers

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. Detaillierte Informationen dazu erhalten 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.

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

***Um einen Jobserver und seine Funktionen zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **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

- Stammdaten eines Jobservers auf Seite 72
- Festlegen der Serverfunktionen auf Seite 75

### Verwandte Themen

- Einrichten des Synchronisationsservers auf Seite 13

# Stammdaten eines Jobservers

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

**Tabelle 23: Eigenschaften eines Jobservers**

| Eigenschaft | Bedeutung |
|---|---|
| Server | Bezeichnung des Jobservers. |
| Vollständiger Servername | Vollständiger Servername gemäß DNS Syntax.<br>Beispiel:<br>`<Name des Servers>.<Vollqualifizierter Domänenname>` |

| Eigenschaft | Bedeutung |
|---|---|
| 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.<br>HINWEIS: Die Eigenschaften **Server ist Cluster** und **Server gehört zu Cluster** schließen einander aus. |
| IP Adresse (IPv6) | Internet Protokoll Version 6 (IPv6)-Adresse des Servers. |
| IP Adresse (IPv4) | Internet Protokoll Version 4 (IPv4)-Adresse des Servers. |
| Kopierverfahren (Quellserver) | Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Quelle einer Kopieraktion ist. Derzeit werden nur Kopierverfahren über die Programme "Robocopy" und "rsync" unterstützt.<br>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.<br>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. |

| Eigenschaft | Bedeutung |
| --- | --- |
| Queue | Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen. |
| Serverbetriebssystem | Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte "Win32", "Windows", "Linux" und "Unix". Ist die Angabe leer, wird "Win32" angenommen. |
| Angaben zum Dienstkonto | Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen. |
| One Identity Manager Service installiert | 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.<br>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.<br>Den Dienst können Sie mit entsprechenden administrativen Rechten im Programm "Job Queue Info" stoppen und starten. |
| kein automatisches Softwareupdate | Angabe, ob die von der automatischen Softwareaktualisierung auszuschließen sind.<br>HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren. |
| Softwareupdate läuft | Angabe, ob gerade eine Softwareaktualisierung ausgeführt wird. |
| Serverfunktion | Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt. |

### Verwandte Themen

- Festlegen der Serverfunktionen auf Seite 75

# 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 24: 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.<br>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. Für ein Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion. |
| 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. |
| SharePoint Online Konnektor | Server, auf dem der SharePoint Online Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem SharePoint Online aus. |

### Verwandte Themen

- Stammdaten eines Jobservers auf Seite 72

# Zielsystemverantwortliche

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

## 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 25: Standardanwendungsrolle für Zielsystemverantwortliche**

| Benutzer | Aufgaben |
|---|---|
| Zielsystemverantwortliche | Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme \| G Suite** oder einer untergeordneten Anwendungsrolle zugewiesen sein.<br><br>Benutzer mit dieser Anwendungsrolle:<br><br>• Übernehmen die administrativen Aufgaben für das Zielsystem.<br>• Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen.<br>• Bearbeiten Kennwortrichtlinien für das Zielsystem.<br>• Bereiten Systemberechtigungen zur Aufnahme in den IT Shop vor.<br>• Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.<br>• Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. |

| Benutzer | Aufgaben |
| --- | --- |
| | • 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.

- Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Zielsysteme | G Suite** zu.
- Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.

6. Speichern Sie die Änderungen.
7. Weisen Sie der Anwendungsrolle die Personen zu, die berechtigt sind, die Kunden-Umgebung im One Identity Manager zu bearbeiten.

## Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer G Suite auf Seite 7

# Fehlerbehebung

## Neu angelegte 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 Nachbehandlung ausstehender Objekte auf Seite 33.

   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: Konfigurationsparameter für die Verwaltung einer G Suite

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

**Tabelle 26: 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\ | Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um |

| Konfigurationsparameter | Bedeutung bei Aktivierung |
|---|---|
| MailTemplateAccountName | Benutzer mit den initialen Anmeldeinformationen (Name des Benutzerkontos) zu versorgen. Es wird die Mailvorlage "Person - Erstellung neues Benutzerkonto" verwendet. |
| TargetSystem\GoogleApps\Accounts\ InitialRandomPassword\SendTo\ MailTemplatePassword | Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den initialen Anmeldeinformationen (initiales 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 |

| Konfigurationsparameter | Bedeutung bei Aktivierung |
|---|---|
| | 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 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: 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 27: 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: Verarbeitung von Systemobjekten

Folgende Tabelle beschreibt die zulässigen Verarbeitungsmethoden für die Schematypen der G Suite und benennt notwendige Einschränkungen bei der Verarbeitung der Systemobjekte.

**Tabelle 28: 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 |

# 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 besuchen Sie https://www.oneidentity.com/company/contact-us.aspx oder rufen Sie + 1-800-306-9329 an.

## 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

## M



## O



## P



## R



## S

## T



## V



## W



## Z