



One Identity Manager 9.1.2

Administrationshandbuch für das Zielsystem-Basismodul

Copyright 2023 One Identity LLC.

ALLE RECHTE VORBEHALTEN.

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

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

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

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

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


Patente

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

Marken

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

Legende

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

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

One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul
Aktualisiert - 20. November 2023, 11:22 Uhr

Die aktuellsten Versionen der Produktdokumentation finden Sie unter [One Identity Manager Dokumentation](#).

Inhalt

Grundlagen zur Behandlung von Personen und Benutzerkonten	5
Administration von Personen und Benutzerkonten	5
Behandlung von Personen und Benutzerkonten	7
Verwenden von Kontendefinitionen zum Erzeugen von Benutzerkonten	10
Kontendefinitionen und Automatisierungsgrade	11
Zuweisen der Kontendefinitionen an Personen	13
Ermitteln der gültigen IT Betriebsdaten für die Zielsysteme	13
IT Betriebsdaten der One Identity Manager Standardkonfiguration	15
Zentrales Benutzerkonto einer Person	17
Standard-E-Mail-Adresse einer Person	18
Ändern von Personenstammdaten	19
Bildungsregeln und Prozesse für den Einsatz von Kontendefinitionen	20
Beispiele für den Einsatz mehrerer Kontendefinitionen innerhalb eines Zielsystemtyps	20
Automatische Zuordnung von Personen zu Benutzerkonten	23
Konfigurieren der automatischen Personenzuordnung	24
Bearbeiten der Suchkriterien für die automatische Personenzuordnung	25
Suchkriterien für die Personenzuordnung definieren	26
Personen suchen und direkt an Benutzerkonten zuordnen	29
Anpassen der Skripte für die automatische Personenzuordnung	31
Deaktivieren und Löschen von Personen und Benutzerkonten	33
Zeitweilige Deaktivierung von Personen	34
Dauerhafte Deaktivierung von Personen	35
Verzögertes Löschen von Personen	37
Deaktivieren und Löschen über Kontendefinitionen	38
Behandlung von Gruppenmitgliedschaften	41
Der Unified Namespace	44
Abbildung der Zielsystemobjekte im Unified Namespace	44
Besonderheiten bei der Abbildung von Objekteigenschaften	50
One Identity Manager Benutzer für die Verwaltung von Zielsystemen im Unified Namespace	51

Unified Namespace Objekte anzeigen	52
Berichte über ein Zielsystem im Unified Namespace	52
Berichte über alle Zielsysteme im Unified Namespace	56
Über uns	57
Kontaktieren Sie uns	57
Technische Supportressourcen	57
Index	58

Grundlagen zur Behandlung von Personen und Benutzerkonten

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

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

- Personen erhalten ihre Benutzerkonten automatisch über One Identity Manager Kontendefinitionen.
- Beim Einfügen eines Benutzerkontos in den One Identity Manager wird automatisch eine vorhandene Person ermittelt und zugeordnet oder im Bedarfsfall eine neue Person erstellt.
- Personen und Benutzerkonten werden im One Identity Manager manuell erfasst und einander zugeordnet.

Administration von Personen und Benutzerkonten

Die Anforderungen an die Benutzerverwaltung in einem Unternehmen sind oft nicht nur in den vorhandenen Zielsystemtypen unterschiedlich, sondern auch in den einzelnen Zielsystemen eines Zielsystemtyps.

Die Anforderungen an die Administration der Benutzerkonten können beispielsweise folgendermaßen aussehen:

Zielsystemtyp Active Directory mit Microsoft Exchange

- In der Domäne A soll automatisch für jede interne Person ein Benutzerkonto erzeugt werden. Die Informationen zum Container und Homeserver richten sich nach der Abteilung und dem Standort der Person. Jedes Benutzerkonto der Domäne erhält automatisch ein Microsoft Exchange Postfach.
- In der Domäne B werden die Benutzerkonten unabhängig von Personendaten verwaltet. Microsoft Exchange Postfächer können nur über ein Bestellverfahren vergeben werden.

Zielsystemtyp HCL Domino

- Alle Personen der Abteilung "Vertrieb" erhalten automatisch ein HCL Domino Postfach. Die Personen der anderen Abteilungen können ein HCL Domino Postfach bestellen. Die Eigenschaften des HCL Domino Postfaches werden abhängig von der Abteilung der Person ermittelt.

Zielsystemtyp SAP R/3

- Alle Personen der Personalabteilung erhalten automatisch ein Benutzerkonto im SAP Mandanten 101.
- Die Personen der Abteilung "Bestellwesen" erhalten automatisch ein Benutzerkonto im SAP Mandanten 102, sobald ihnen die entsprechende Rolle zugewiesen wurde.
- Die Benutzerkonten für den SAP Mandanten 103 werden ausschließlich über ein Bestellverfahren vergeben.

Für die Zuordnung von Benutzerkonten zu Personen bedient sich der One Identity Manager verschiedener Mechanismen.

Initiale Zuordnung von Benutzerkonten

Die Benutzerkonten werden durch eine Synchronisation zunächst initial aus einem Zielsystem in den One Identity Manager eingelesen. Dabei kann bereits die automatische Zuordnung der Benutzerkonten zu bestehenden Personen erfolgen. Gegebenenfalls können neue Personen erzeugt werden und den Benutzerkonten zugeordnet werden. Die Kriterien für diese automatische Zuordnung eines Benutzerkontos zu einer Person werden unternehmensspezifisch definiert. Nach einer Prüfung der Benutzerkonten kann über Kontendefinitionen der Umfang der Eigenschaften, die eine Person an ihr Benutzerkonto vererbt, gesteuert werden. Dadurch wird bei Änderungen am System ein Verlust von Benutzerkonten vermieden. Die Prüfung der Benutzerkonten kann manuell oder skriptgesteuert erfolgen.

Zuordnung von Benutzerkonten im laufenden Betrieb

Um im laufenden Betrieb Benutzerkonten an Personen zu vergeben, verwendet der One Identity Manager Kontendefinitionen. Kontendefinitionen können für jedes Zielsystem der eingesetzten Zielsystemtypen erzeugt werden, beispielsweise für die unterschiedlichen Domänen einer Active Directory-Umgebung oder die einzelnen Mandanten eines SAP R/3-Systems. Um sicherzustellen, dass beispielsweise ein Microsoft Exchange Postfach erst

erzeugt wird, wenn auch ein Active Directory Benutzerkonto vorhanden ist, erhalten die Kontendefinitionen eine Priorität.

Durch die direkte Zuweisung der Kontendefinition an eine Person oder durch Zuweisung der Kontendefinition an Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen kann eine Person über die integrierten Vererbungsmechanismen ein Benutzerkonto erhalten. Kontendefinitionen können automatisch an alle Personen eines Unternehmens zugewiesen werden, unabhängig von ihrer Zugehörigkeit zu Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen. Es ist im One Identity Manager möglich die Kontendefinitionen als bestellbare Artikel dem IT Shop zuzuordnen. Der Abteilungsleiter kann dann für seine Mitarbeiter Benutzerkonten über das Web Portal bestellen.

Behandlung der Benutzerkonten und Personendaten bei Deaktivierung

Der Umgang mit Personendaten, vor allem beim dauerhaften oder zeitweisen Ausscheiden einer Person aus dem Unternehmen, wird in den einzelnen Unternehmen unterschiedlich gehandhabt. Es gibt Unternehmen, die Personendaten nie löschen, sondern diese nur deaktivieren, wenn die Person das Unternehmen verlässt. Andere Unternehmen wollen die Personendaten löschen, jedoch erst dann, wenn sichergestellt ist, dass alle Benutzerkonten der Person gelöscht wurden.

Behandlung von Personen und Benutzerkonten

Die Anforderungen an die Benutzerverwaltung in einem Unternehmen sind oft nicht nur in den vorhandenen Zielsystemtypen unterschiedlich, sondern auch in den einzelnen Zielsystemen eines Zielsystemtyps. Selbst innerhalb eines Zielsystems kann es für unterschiedliche Benutzergruppen unterschiedliche Regeln geben. So können beispielsweise in den einzelnen Domänen innerhalb einer Active Directory-Umgebung unterschiedliche Regeln zur Vergabe von Benutzerkonten gelten.

Eine Anforderung könnte beispielsweise wie folgt aussehen:

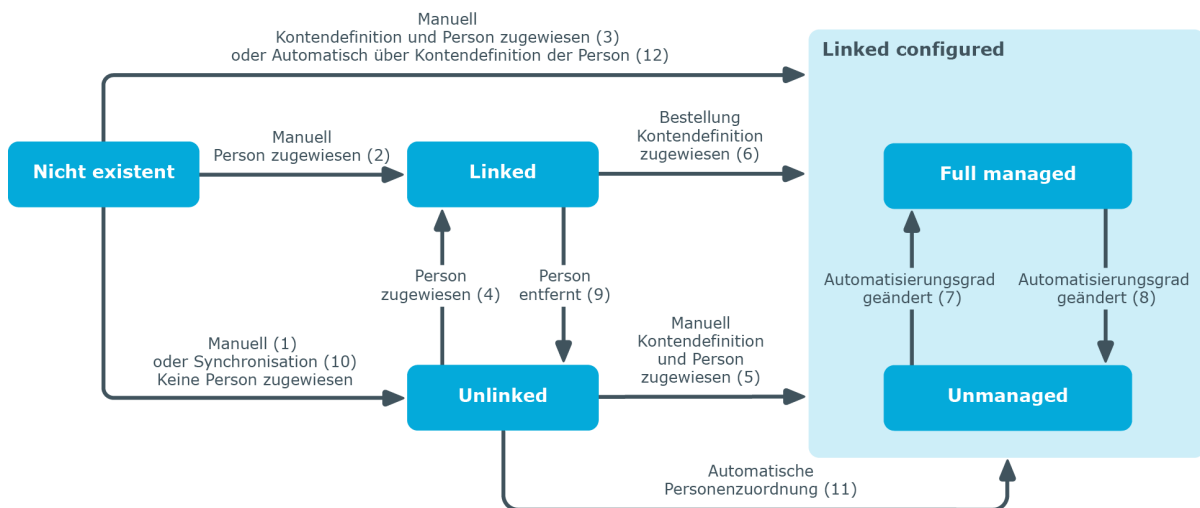
- In der Domäne A werden die Benutzerkonten unabhängig von Personendaten verwaltet.
- In der Domäne B werden die Benutzerkonten mit einer Person verbunden. Es ist jedoch keine Übernahme der Personenstammdaten an die Benutzerkonten erwünscht.
- In der Domäne C soll automatisch für jede interne Person ein Benutzerkonto erzeugt werden. Die Informationen zum Container, Homeserver und Profilservers richten sich nach der Abteilung und dem Standort der Person.

Um die einzelnen Anforderungen an die Benutzerverwaltung zu erfüllen, können die Benutzerkonten zunächst in Kategorien eingeteilt werden:

- **Unlinked** (nicht verbunden): Die Benutzerkonten haben keine Verbindung zur Person.
- **Linked** (verbunden): Die Benutzerkonten haben eine Verbindung zur Person.
- **Linked configured** (verbunden mit Konfiguration der Verbindung): Die Benutzerkonten haben eine Verbindung zur Person. Über eine Kontendefinition und deren Automatisierungsgrade kann die Auswirkung der Verbindung und der Umfang der vererbten Eigenschaften der Person an die Benutzerkonten konfiguriert werden.
- Der One Identity Manager liefert eine Standardkonfiguration mit den Automatisierungsgraden:
 - **Unmanaged**: Die Benutzerkonten haben eine Zuordnung zur Person, erben jedoch keine weiteren Eigenschaften der Person.
 - **Full managed**: Die Benutzerkonten haben eine Zuordnung zur Person und erben die Eigenschaften der Personen.

Die folgende Abbildung soll die möglichen Übergänge der Benutzerkonten verdeutlichen. Dabei werden die im One Identity Manager integrierten Standardmechanismen zur Verwaltung der Personen und der Benutzerkonten dargestellt.

Abbildung 1: Übergangszustände eines Benutzerkontos



Manuelles Einfügen eines Benutzerkontos

- Fall 1: Um ein Benutzerkonto unabhängig von Personendaten zu verwalten, wird das Benutzerkonto manuell angelegt und keine Person zugewiesen. Das Benutzerkonto ist nicht mit einer Person verbunden und hat damit den Zustand **Unlinked**.
- Fall 2: Wird das Benutzerkonto bereits beim manuellen Einfügen mit einer Person verbunden geht das Benutzerkonto in den Zustand **Linked** über.
- Fall 3: Wird beim Anlegen des Benutzerkontos bereits eine Person zugewiesen und gleichzeitig eine Kontendefinition zugewiesen, geht das Benutzerkonto in den Zustand **Linked configured** über. Abhängig vom verwendeten

Automatisierungsgrad wird der Zustand **Linked configured: Unmanaged** oder **Linked configured: Full managed** erreicht.

Bearbeiten eines bestehenden Benutzerkontos

- Fall 4: Wird einem bestehenden Benutzerkonto manuell eine Person zugeordnet, geht das Benutzerkonto aus dem Zustand **Unlinked** in den Zustand **Linked** über.
- Fall 5: Wird einem bestehenden Benutzerkonto manuell eine Person zugeordnet und gleichzeitig eine Kontendefinition zugewiesen, geht das Benutzerkonto aus dem Zustand **Unlinked** in den Zustand **Linked configured** über. Abhängig vom verwendeten Automatisierungsgrad wird der Zustand **Linked configured: Unmanaged** oder **Linked configured: Full managed** erreicht.
- Fall 6: Bei der Inbetriebnahme des One Identity Manager können für bestehende Benutzerkonten, die mit Personen verbunden sind (Zustand **Linked**) IT Shop Bestellungen erzeugt werden. Dabei wird eine Kontendefinition zugewiesen und das Benutzerkonto geht in den Zustand **Linked configured**. Abhängig vom verwendeten Automatisierungsgrad wird der Zustand **Linked configured: Unmanaged** oder **Linked configured: Full managed** erreicht.

Ändern des Automatisierungsgrades

- Fall 7 und Fall 8: Durch Anpassung des Automatisierungsgrades kann ein bestehendes Benutzerkonto vom Zustand **Linked configured: Unmanaged** in den Zustand **Linked configured: Full managed** übergehen und umgekehrt. Der Automatisierungsgrad kann dabei nur für Benutzerkonten, die mit einer Person verbunden sind, geändert werden.

Entfernen von Personenzuordnungen

- Fall 9: Durch das Entfernen des Personeneintrages in einem verbundenen Benutzerkonto (**Linked**), geht das Benutzerkonto in den Zustand **Unlinked** über.

HINWEIS: Der Personeneintrag kann von Benutzerkonten im Zustand **Linked configured** nicht entfernt werden, solange die Person die Kontendefinition besitzt.

Behandlung der Benutzerkonten bei der Synchronisation

- Fall 10: Durch eine Synchronisation der Datenbank mit einem Zielsystem werden die Benutzerkonten immer ohne Personenzuordnung angelegt und haben somit initial den Zustand **Unlinked**. Anschließend kann die Zuweisung von Personen vorgenommen werden. Diese Zuweisung kann manuell oder über die automatische Personenzuordnung per Prozessverarbeitung erfolgen.

Automatische Personenzuordnung zu bestehenden Benutzerkonten

- Fall 11: An Benutzerkonten im Zustand **Unlinked** kann der One Identity Manager automatisch Personen zuordnen. Wenn dem Zielsystem eine Kontendefinition zugewiesen ist, wird diese Kontendefinition auch an die Personen zugewiesen.

Abhängig vom verwendeten Automatisierungsgrad wird der Zustand **Linked configured: Unmanaged** oder **Linked configured: Full managed** erreicht. Die automatische Personenzuordnung kann auf das Einfügen oder Aktualisieren von Benutzerkonten durch eine Synchronisation oder das manuelle Einfügen eines Benutzerkontos folgen. Weitere Informationen finden Sie unter [Automatische Zuordnung von Personen zu Benutzerkonten](#) auf Seite 23.

Automatische Erzeugung von Benutzerkonten über Kontendefinitionen

- Fall 12: Um im laufenden Betrieb Benutzerkonten automatisch an Personen zu vergeben, werden Kontendefinitionen eingesetzt. 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. Der Automatisierungsgrad wird angepasst auf den Standardautomatisierungsgrad und das Benutzerkonto hat den Zustand **Linked configured**. Abhängig vom verwendeten Automatisierungsgrad wird der Zustand **Linked configured: Unmanaged** oder **Linked configured: Full managed** erreicht. Weitere Informationen finden Sie unter [Kontendefinitionen und Automatisierungsgrade](#) auf Seite 11.

Entfernen von Kontendefinitionen

- Wenn die Zuweisung einer Kontendefinition von einer Person entfernt wird, wird das verbundene Benutzerkonto gelöscht.
- Über die Aufgabe **Entferne Kontendefinition** am Benutzerkonto können Sie das Benutzerkonto wieder in den Zustand **Linked** zurücksetzen. Dabei wird die Kontendefinition vom Benutzerkonto und von der Person entfernt. Das Benutzerkonto bleibt über diese Aufgabe erhalten, wird aber nicht mehr über die Kontendefinition verwaltet. Die Aufgabe entfernt nur Kontendefinitionen, die direkt zugewiesen sind (XOrigin=1).

Verwenden von Kontendefinitionen zum Erzeugen von Benutzerkonten

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

Aus den Personenstammdaten resultieren die Daten für das Benutzerkonto im jeweiligen Zielsystem. Die Personen müssen ein zentrales Benutzerkonto besitzen. 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.

Kontendefinitionen und Automatisierungsgrade

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.

Kontendefinitionen können für jedes Zielsystem der eingesetzten Zielsystemtypen erzeugt werden, beispielsweise für die unterschiedlichen Domänen einer Active Directory-Umgebung oder die einzelnen Mandanten eines SAP R/3-Systems. Eine Kontendefinition ist immer für ein Zielsystem gültig. Für ein Zielsystem können jedoch mehrere Kontendefinitionen definiert werden. Welche Kontendefinition verwendet wird, entscheidet sich beim Erzeugen eines Benutzerkontos für eine Person. Um sicherzustellen, dass beispielsweise ein Microsoft Exchange Postfach erst erzeugt wird, wenn auch ein Active Directory Benutzerkonto vorhanden ist, können Abhängigkeiten zwischen Kontendefinitionen festgelegt werden.

An einer Kontendefinition wird festgelegt, welche Automatisierungsgrade genutzt werden können. Es können mehrere Automatisierungsgrade erstellt werden. Der Automatisierungsgrad entscheidet über den Umfang der vererbten Eigenschaften der Person an ihre Benutzerkonten. 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. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Person werden initial die Personeneigenschaften übernommen. Werden die Personeneigenschaften zu einem späteren Zeitpunkt geändert, dann werden diese Änderungen an das Benutzerkonto weitergereicht.

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.

Für jede Kontendefinition wird ein Automatisierungsgrad als Standard festgelegt. Dieser Standardautomatisierungsgrad wird bei der automatischen Erzeugung neuer Benutzerkonten zur Ermittlung der gültigen IT Betriebsdaten genutzt. 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 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.

Für jede Kontendefinition wird festgelegt, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf Zuweisung der Kontendefinition selbst auswirken soll.

- Solange eine Kontendefinition für eine Person wirksam ist, behält die Person ihre verbundenen Benutzerkonten. Die Zuweisung von Kontendefinitionen an deaktivierte Personen kann beispielsweise gewünscht sein, um bei späterer Aktivierung der Person sicherzustellen, dass sofort alle erforderlichen Berechtigungen ohne Zeitverlust zur Verfügung stehen.
- Ist die Zuweisung einer Kontendefinition nicht mehr wirksam oder wird die Kontendefinition von der Person entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht.

Zusätzlich wird für jeden Automatisierungsgrad festgelegt, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf ihre Benutzerkonten und die Gruppenmitgliedschaften auswirken soll.

- 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!

Zuweisen der Kontendefinitionen an Personen

Kontendefinitionen werden an die Personen des Unternehmens zugewiesen.

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

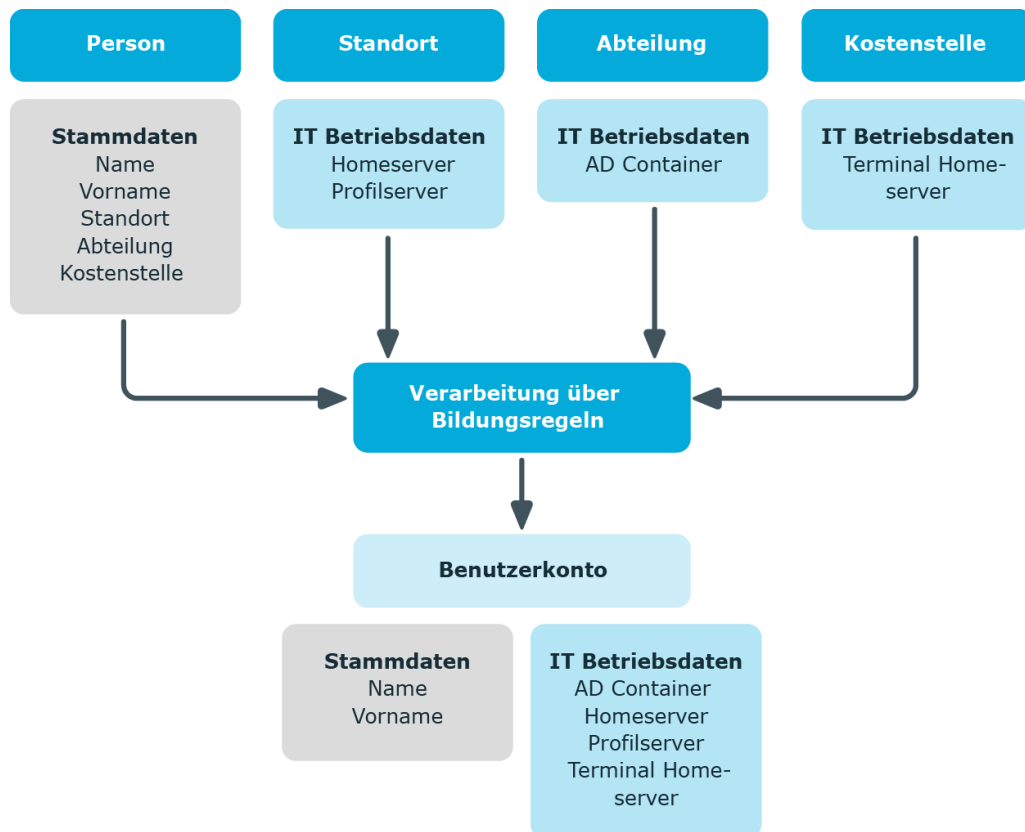
Kontendefinitionen können automatisch an alle Personen eines Unternehmens zugewiesen werden. Es ist möglich, die Kontendefinitionen als bestellbare Produkte dem IT Shop zuzuordnen. Der Abteilungsleiter kann dann für seine Mitarbeiter Benutzerkonten über das Web Portal bestellen. Zusätzlich ist es möglich,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

Ermitteln der gültigen IT Betriebsdaten für die Zielsysteme

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

Die Prozessabläufe für die automatische Zuordnung der IT Betriebsdaten zu den Benutzerkonten einer Person innerhalb des One Identity Manager sollen anhand der nachfolgenden Abbildung veranschaulicht werden.

Abbildung 2: Abbildung der IT Betriebsdaten auf ein Benutzerkonto



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 Domäne A. Zusätzlich erhalten einige Personen der Abteilung A administrative Benutzerkonten in der Domäne A.

Erstellen Sie eine Kontendefinition A für die Standardbenutzerkonten der Domäne A und eine Kontendefinition B für die administrativen Benutzerkonten der Domäne 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 Domäne 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.

IT Betriebsdaten der One Identity Manager Standardkonfiguration

Die IT Betriebsdaten, die in der Standardkonfiguration des One Identity Manager für das automatische Erzeugen oder Ändern von Benutzerkonten und Postfächer für eine Person in den Zielsystemen verwendet werden, sind in der nachfolgenden Tabelle aufgeführt.

HINWEIS: Die IT Betriebsdaten sind abhängig vom Zielsystem und sind in den One Identity Manager Modulen enthalten. Die Daten stehen erst zur Verfügung, wenn die Module installiert sind.

Tabelle 1: Zielsystemtyp-abhängige IT Betriebsdaten

Zielsystemtyp	IT Betriebsdaten
Active Directory	Container Homeserver Profilservers Terminal Homeserver Terminal Profilservers Gruppen erbbbar Identität Privilegiertes Benutzerkonto
Microsoft Exchange	Postfachdatenbank
LDAP	Container Gruppen erbbbar Identität Privilegiertes Benutzerkonto
Domino	Server Zertifikat Vorlage der Postdatei Identität
SharePoint	Authentifizierungsmodus

Zielsystemtyp	IT Betriebsdaten
	<ul style="list-style-type: none"> Gruppen erbbar Rollen erbbar Identität Privilegiertes Benutzerkonto
SharePoint Online	<ul style="list-style-type: none"> Gruppen erbbar Rollen erbbar Privilegiertes Benutzerkonto Authentifizierungsmodus
Kundendefinierte Zielsysteme	<ul style="list-style-type: none"> Container (je Zielsystem) Gruppen erbbar Identität Privilegiertes Benutzerkonto
Azure Active Directory	<ul style="list-style-type: none"> Gruppen erbbar Administratorrollen erbbar Abonnements erbbar Unwirksame Dienstpläne erbbar Identität Privilegiertes Benutzerkonto Kennwort bei der nächsten Anmeldung ändern
Cloud Zielsystem	<ul style="list-style-type: none"> Container (je Zielsystem) Gruppen erbbar Identität Privilegiertes Benutzerkonto
Unix-basierte Zielsysteme	<ul style="list-style-type: none"> Login-Shell Gruppen erbbar Identität Privilegiertes Benutzerkonto
Oracle E-Business Suite	<ul style="list-style-type: none"> Identität Gruppen erbbar Privilegiertes Benutzerkonto
SAP R/3	<ul style="list-style-type: none"> Identität Gruppen erbbar

Zielsystemtyp	IT Betriebsdaten
	Rollen erbbbar Profile erbbbar Strukturelle Profile erbbbar Privilegiertes Benutzerkonto
Exchange Online	Gruppen erbbbar
Privileged Account Management	Authentifizierungsanbieter Gruppen erbbbar Identität Privilegiertes Benutzerkonto
Google Workspace	Organisation Gruppen erbbbar Produkte und SKUs erbbbar Admin-Rollen-Zuordnungen erbbbar Identität Privilegiertes Benutzerkonto Kennwort bei der nächsten Anmeldung ändern
OneLogin	Rollen erbbbar Identität Privilegiertes Benutzerkonto Lizenzierungsstatus OneLogin Gruppe

Zentrales Benutzerkonto einer Person

Tabelle 2: Konfigurationsparameter für die Bildung der zentralen Benutzerkonten

Konfigurationsparameter	Bedeutung
QER Person CentralAccountGlobalUnique	Legt fest, wie das zentrale Benutzerkonto abgebildet wird. Ist der Konfigurationsparameter aktiviert, erfolgt die Bildung des zentralen Benutzerkonto einer Person eindeutig bezogen auf die zentralen Benutzerkonten aller Personen und die Benutzerkontennamen aller erlaubten Zielsysteme.

Konfigurationsparameter Bedeutung

Ist der Konfigurationsparameter nicht aktiviert, erfolgt die Bildung nur eindeutig bezogen auf die zentralen Benutzerkonten aller Personen.

Das zentrale Benutzerkonto einer Person wird zur Bildung des Anmeldenamens der Benutzerkonten in den aktivierten Zielsystemen herangezogen. Das zentrale Benutzerkonto wird weiterhin bei der Anmeldung an den Werkzeugen des One Identity Manager genutzt. In der Standardinstallation des One Identity Manager wird das zentrale Benutzerkonto aus dem Vornamen und dem Nachnamen der Person gebildet. Ist nur eine dieser Eigenschaften bekannt, wird diese zur Bildung des zentralen Benutzerkontos genutzt. Der One Identity Manager prüft in jedem Fall, ob es bereits ein zentrales Benutzerkonto mit dem ermittelten Wert gibt. Ist dies der Fall, wird eine fortlaufende Nummerierung, beginnend mit 1, an den ursprünglichen Wert angehängt.

Tabelle 3: Beispiel für die Bildung des zentralen Benutzerkontos

Vorname	Nachname	Zentrales Benutzerkonto
Clara		CLARA
	Harris	HARRIS
Clara	Harris	CLARAH
Clara	Harrison	CLARAH1

Verwandte Themen

- [Standard-E-Mail-Adresse einer Person](#) auf Seite 18
- [Ändern von Personenstammdaten](#) auf Seite 19

Standard-E-Mail-Adresse einer Person

Die Standard-E-Mail-Adresse der Person wird auf die Postfächer in den aktivierten Zielsystemen abgebildet. In der Standardinstallation des One Identity Manager wird die Standard-E-Mail-Adresse aus dem zentralen Benutzerkonto der Person und der Standardmaildomäne der aktivierten Zielsysteme gebildet.

Die Standardmaildomäne wird aus dem Konfigurationsparameter **QER | Person | DefaultMailDomain** ermittelt.

- Aktivieren Sie im Designer den Konfigurationsparameter und tragen Sie die Bezeichnung der Standardmaildomäne als Wert ein.

Verwandte Themen

- [Zentrales Benutzerkonto einer Person](#) auf Seite 17
- [Ändern von Personenstammdaten](#) auf Seite 19

Ändern von Personenstammdaten

Nachfolgend wird nur auf die Personenstammdaten eingegangen, deren Änderungen in der One Identity Manager Standardinstallation Auswirkungen auf die Benutzerkonten einer Person mit dem Automatisierungsgrad **Full managed** haben.

Allgemeine Änderungen

Dieser Prozess betrifft alle Änderungen der Daten in Bezug auf Telefonnummer, Faxnummer, Mobiltelefon, Straße, PLZ oder Ort einer Person und ändert die Daten in den Benutzerkonten der Zielsysteme, die der Person zugeordnet sind, sofern diese Daten im jeweiligen Zielsystem abgebildet sind.

Namensänderung einer Person

Namensänderungen einer Person beeinflussen die Bildung des zentralen Benutzerkontos einer Person. Nach der Bildungsregel wird aus Vorname und Nachname das zentrale Benutzerkonto gebildet. Das zentrale Benutzerkonto wird in einigen Zielsystemen als Vorlage für die Bildung der Anmeldenamens der Benutzerkonten verwendet. Weitere überschreibende Bildungsregeln steuern bei der Anlage eines Benutzerkontos beispielsweise die Bildung für das Homeverzeichnis und das Profilverzeichnis aus dem zentralen Benutzerkonto, die auch bei Namensänderungen angepasst werden.

Innerbetrieblicher Wechsel einer Person

Der innerbetriebliche Wechsel wird über die Änderungen des Standortes oder der Abteilung gesteuert. Im One Identity Manager werden damit die administrativen Abläufe für die Veränderung der zielsystemabhängigen IT Betriebsdaten, beispielsweise Domäne, Homeserver oder Profilservers, automatisiert. Aufgrund der systembedingten Unterschiede der Zielsysteme hinsichtlich der notwendigen Aktionen für einen Abteilungswechsel gibt es für jedes Zielsystem andere Subprozesse.

Verwandte Themen

- [Zentrales Benutzerkonto einer Person](#) auf Seite 17
- [Standard-E-Mail-Adresse einer Person](#) auf Seite 18

Bildungsregeln und Prozesse für den Einsatz von Kontendefinitionen

Zur Abbildung der IT Betriebsdaten werden nur die Eigenschaften der Benutzerkonten angeboten, die in der Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Wenn Sie von der Standardinstallation abweichende oder zusätzliche Eigenschaften verwenden wollen, erstellen Sie kundenspezifische Bildungsregeln unter Verwendung dieses Skriptes.

In der Standardinstallation des One Identity Manager ist pro Zielsystemtyp jeweils ein Prozess für die Erstellung von Benutzerkonten über Kontendefinitionen enthalten. Diese Prozesse können Sie als Kopiervorlagen für die unternehmensspezifische Erweiterungen des Verhaltens nutzen.

HINWEIS: Die Prozesse sind in den One Identity Manager Modulen definiert und stehen erst zur Verfügung, wenn die Module installiert sind.

Der Name der Prozesse ist folgendermaßen aufgebaut:

```
<MMM>_PersonHasTSBAccountDef_Autocreate_<Benutzerkontentabelle>
```

wobei:

<MMM> = Kennung des Moduls

<Benutzerkontentabelle> = Tabelle, in der die Benutzerkonten des Zielsystemtyps abgebildet werden

Beispiele für den Einsatz mehrerer Kontendefinitionen innerhalb eines Zielsystemtyps

Sollen in einem Zielsystemtyp mehrere Zielsysteme über Kontendefinitionen verwaltet werden, muss pro Zielsystem eine separate Kontendefinition eingerichtet werden. Bei Zuweisung beider Kontendefinitionen an die Person wird durch die anschließende Skript- und Prozessverarbeitung dafür gesorgt, dass die Person ihre Benutzerkonten in beiden Zielsystemen erhält.

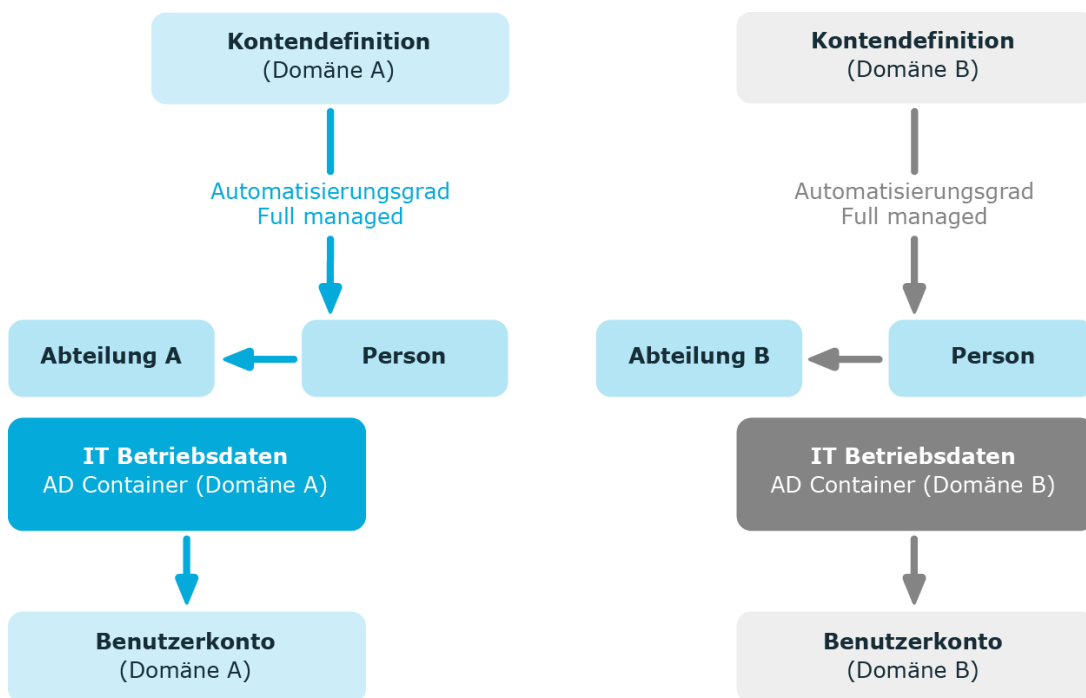
Beispiel: Personen können nur in einer Domäne ein Benutzerkonto besitzen

In einer Active Directory-Umgebung existieren zwei Domänen. Die Personen können nur in einer der beiden Domänen ein Benutzerkonto besitzen. Anhand der IT Betriebsdaten der Abteilung einer Person wird entschieden, ob das Benutzerkonto in Domäne A oder in Domäne B erstellt wird.

Erstellen Sie eine Kontendefinition A für die Domäne A und eine Kontendefinition B für die Domäne B und weisen Sie den Automatisierungsgrad **Full managed** zu. Dieser Automatisierungsgrad nutzt zur Ermittlung der IT Betriebsdaten die Standardbildungsregeln des One Identity Manager. In der Abbildungsvorschrift der IT Betriebsdaten für beide Kontendefinitionen legen Sie die Eigenschaft **Abteilung** zur Ermittlung der gültigen IT Betriebsdaten fest.

Gehört die Person zur Abteilung A, dann erhält Sie, beispielsweise per dynamischer Zuweisung, die Kontendefinition A und daraus resultierend ein Benutzerkonto in Domäne A. Gehört die Person zur Abteilung B, dann wird ihr die Kontendefinition B zugeteilt und sie erhält ein Benutzerkonto in Domäne B.

Abbildung 3: Erzeugung von Benutzerkonten anhand von Kontendefinitionen

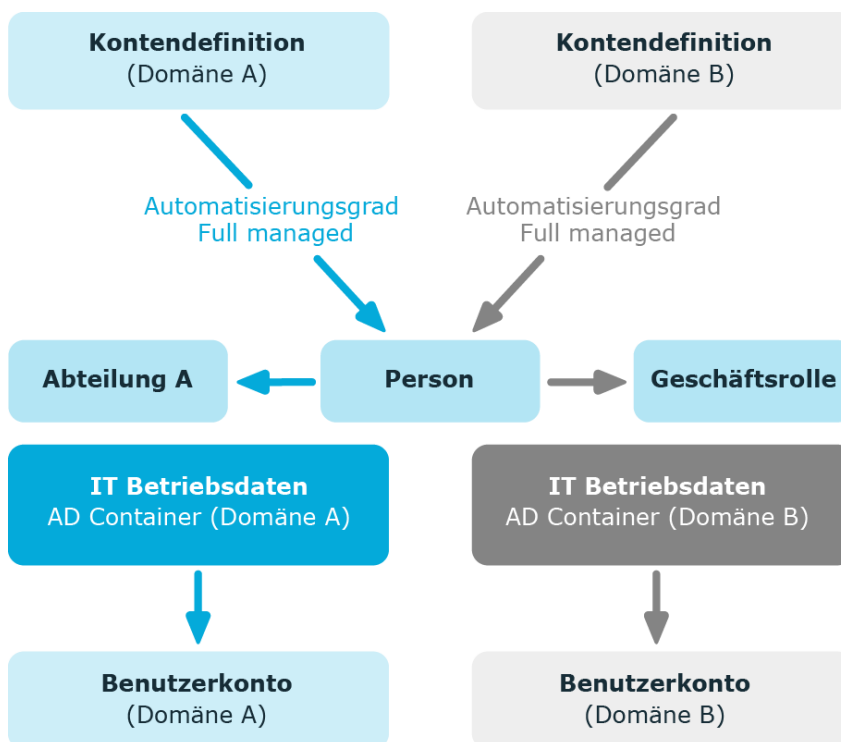


Beispiel: Personen können in mehreren Domänen ein Benutzerkonto besitzen

In einer Active Directory-Umgebung existieren zwei Domänen. Die Personen können in beiden Domänen ein Benutzerkonto besitzen. Das Benutzerkonto in Domäne A

erhält die IT Betriebsdaten über die Abteilung einer Person. Das Benutzerkonto in Domäne B erhält die IT Betriebsdaten über die primäre Geschäftsrolle einer Person. Erstellen Sie eine Kontendefinition A für die Domäne A und eine Kontendefinition B für die Domäne B und weisen Sie den Automatisierungsgrad **Full managed** zu. Der Automatisierungsgrad **Full managed** nutzt zur Ermittlung der IT Betriebsdaten die Standardbildungsregeln des One Identity Manager. In der Abbildungsvorschrift der IT Betriebsdaten für Kontendefinition A legen Sie die Eigenschaft **Abteilung** zur Ermittlung der gültigen IT Betriebsdaten fest. In der Abbildungsvorschrift der IT Betriebsdaten für Kontendefinition B legen Sie die Eigenschaft **Geschäftsrolle** zur Ermittlung der gültigen IT Betriebsdaten fest.

Abbildung 4: Erzeugung von Benutzerkonten anhand von Kontendefinitionen



Automatische Zuordnung von Personen zu Benutzerkonten

Durch die automatische Personenzuordnung können

- vorhandene Personen an Benutzerkonten zugeordnet werden
- Personenstammdaten anhand vorhandener Benutzerkonten erzeugt werden

Durch eine Synchronisation werden die Benutzerkonten zunächst initial aus einem Zielsystem in den One Identity Manager eingelesen. Durch anschließende Skript- und Prozessverarbeitung kann die automatische Zuordnung der Benutzerkonten zu bestehenden Personen erfolgen. Gegebenenfalls können neue Personen anhand vorhandener Benutzerkonten erzeugt und den Benutzerkonten zugeordnet werden. Dieses Vorgehen ist jedoch nicht das Standardverfahren für den One Identity Manager. Das Verfahren können Sie einsetzen, um bei der Synchronisation aus den bereits vorhandenen Benutzerkonten eines Zielsystems Personendatensätze zu erstellen.

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

Die Kriterien für die automatische Zuordnung eines Benutzerkontos zu einer Person werden unternehmensspezifisch definiert. Personen können bei Bedarf anhand einer Vorschlagsliste direkt an vorhandene Benutzerkonten zugeordnet werden.

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

- Aktivieren Sie im Designer die Konfigurationsparameter für die automatische Zuordnung der Personen zu Benutzerkonten und wählen Sie den gewünschten Modus aus.
- Definieren Sie die Suchkriterien für die Personenzuordnung.
- Sollen durch die automatische Personenzuordnung verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen, dann weisen Sie dem Zielsystem eine Kontendefinition zu. Stellen Sie sicher, dass der Automatisierungsgrad, der verwendet werden soll, als Standardautomatisierungsgrad eingetragen ist.

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

Verwandte Themen

- [Behandlung von Personen und Benutzerkonten](#) auf Seite 7
- [Konfigurieren der automatischen Personenzuordnung](#) auf Seite 24

- [Bearbeiten der Suchkriterien für die automatische Personenzuordnung](#) auf Seite 25
- [Anpassen der Skripte für die automatische Personenzuordnung](#) auf Seite 31

Konfigurieren der automatischen Personenzuordnung

In der One Identity Manager Standardinstallation wird die automatische Zuordnung von Personen zu Benutzerkonten über Konfigurationsparameter gesteuert und ist somit global für einen Zielsystemtyp wirksam. Es wird dabei zwischen dem Verhalten bei Synchronisationen und dem Standardverhalten unterschieden.

HINWEIS:

Für die Synchronisation gilt:

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

Außerhalb der Synchronisation gilt:

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

HINWEIS: Die Konfigurationsparameter sind in den One Identity Manager Modulen enthalten und stehen zur Verfügung, wenn die Module installiert sind.

Konfigurationsparameter für die automatische Personenzuordnung:

- **TargetSystem | <Zielsystemtyp> | PersonAutoDefault**
- **TargetSystem | <Zielsystemtyp> | PersonAutoFullSync**

Jeder Konfigurationsparameter kennt die zulässigen Modi:

- **NO:** Es erfolgt keine automatische Zuordnung einer Person zum Benutzerkonto. Dies ist der Standardwert, der auch abgebildet wird, wenn der Konfigurationsparameter nicht aktiv ist.
- **SEARCH:** Ist dem Benutzerkonto keine Person zugeordnet, so wird anhand definierter Kriterien nach der passenden Person gesucht und die gefundene Person dem Benutzerkonto zugeordnet. Wird keine Person gefunden, so wird auch keine neue Person angelegt.
- **CREATE:** Ist dem Benutzerkonto keine Person zugeordnet, wird immer eine neue Person angelegt, einige Eigenschaften initialisiert und die Person dem Benutzerkonto zugeordnet.

| **HINWEIS:** Dieser Modus steht nicht für alle Zielsystemtypen zur Verfügung.

- **SEARCH AND CREATE:** Ist dem Benutzerkonto keine Person zugeordnet, wird anhand definierter Kriterien nach einer passenden Person gesucht und die gefundene Person dem Benutzerkonto zugeordnet. Wird keine Person gefunden, so werden eine neue Person angelegt, einige Eigenschaften initialisiert und die Person dem

Benutzerkonto zugeordnet.

| **HINWEIS:** Dieser Modus steht nicht für alle Zielsystemtypen zur Verfügung.

Wird durch den eingesetzten Modus ein Benutzerkonto mit einer Person verbunden, so erhält das Benutzerkonto durch interne Verarbeitung den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Diesen Automatisierungsgrad können Sie nachträglich ändern.

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 das Zielsystem bekannt, werden die Benutzerkonten mit den Personen verbunden. Es wird jedoch noch keine Kontendefinition zugewiesen. Die Benutzerkonten sind somit im Zustand **Linked** (verbunden).

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

Um die Benutzerkonten über Kontendefinitionen zu verwalten

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

In den Zielsystemtyp-abhängigen Insert/Update-Prozessen der One Identity Manager Standardinstallation werden die Konfigurationsparameter ausgewertet und so der auszuführende Modus ermittelt. Die Namen der entsprechenden Prozessschritte lauten Search and Create Person for Account und Search and Create Person for Account (Fullsync). Um die automatische Personenzuordnung in den einzelnen Zielsystemen eines Zielsystemtyps, beispielsweise den einzelnen Domänen einer Active Directory-Umgebung, unterschiedlich einzusetzen, können Sie diese Prozessschritte als Vorlage nutzen.

Bearbeiten der Suchkriterien für die automatische Personenzuordnung

Die Kriterien für die Personenzuordnung werden an den Zielsystemen definiert. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person

übereinstimmen müssen, damit die Person dem Benutzerkonto zugeordnet werden kann. Die Suchkriterien können Sie durch Formatdefinitionen weiter einschränken.

Das zusammengestellte Suchkriterium wird in XML-Notation in die Spalte **Suchkriterien für die automatische Personenzuordnung** (AccountToPersonMatchingRule) der Zielsystem-Tabelle geschrieben.

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

HINWEIS: Die Objektdefinitionen für Benutzerkonten, auf welche die Suchkriterien angewendet werden können, sind vordefiniert. Sollten Sie weitere Objektdefinitionen benötigen, um beispielsweise die Vorauswahl der Benutzerkonten weiter einzuschränken, erzeugen Sie im Designer die entsprechenden kundenspezifische Objektdefinitionen. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Detaillierte Informationen zum Thema

- [Suchkriterien für die Personenzuordnung definieren](#) auf Seite 26
- [Personen suchen und direkt an Benutzerkonten zuordnen](#) auf Seite 29

Suchkriterien für die Personenzuordnung definieren

Abbildung 5: Suchkriterien für die Personenzuordnung

The screenshot shows the 'Suchkriterien' (Search Criteria) configuration window. It is divided into several sections:

- Suchkriterien:** A tree view on the left shows the hierarchy of search criteria. The selected criterion is 'CentralAccount <-> SAMAccountName'.
- Anwenden auf:** A dropdown menu set to 'Active Directory Benutzerkonten'.
- Spalte an Person:** A dropdown menu set to 'Zentrales Benutzerkonto (CentralAccount)'. A checkbox 'Formatierung anwenden' is checked.
- Spalte am Benutzerkonto:** A dropdown menu set to 'Anmeldename (pre Win2000) [SAMAccountNam]'. A checkbox 'Formatierung anwenden' is checked.
- Format hinzufügen:** A section with radio buttons for 'Verwende alle Zeichen' and 'Verwende Bereich'. The 'Verwende Bereich' option is selected. Below it are input fields for 'Von Position' (set to 1) and 'Anzahl Zeichen' (set to 19).
- Formatierungsvorschau:** A text box showing a preview of the formatted search result: 'Franz jagt im komplett verwahrlosten Taxi quer durch Bayern.'
- Zuordnungen:** A table at the bottom showing suggested assignments. The table has columns for 'Benutzerkonto', 'Person', and 'Auswahl'. The 'Auswahl' column contains 'Person auswählen...' buttons. The table shows 14 'Ohne Personenzuordnung' entries.

Blue arrows on the right side of the screenshot point to the following elements:

- Objekteigenschaften
- Formatregeln
- Zuordnungen

HINWEIS: Der One Identity Manager liefert ein Standardmapping für die Personenzuordnung. Führen Sie die folgenden Schritte nur aus, wenn Sie das Standardmapping unternehmensspezifisch anpassen möchten.

Um ein neues Suchkriterium für die Personenzuordnung zu definieren:

1. Wählen Sie im Manager die Kategorie **Zielsystemtyp > <Zielsystem>**.
2. Wählen Sie in der Ergebnisliste das Zielsystem und führen Sie die Aufgabe **Suchkriterien für die Personenzuordnung definieren** aus.
3. Wählen Sie eine Objektdefinition für das Mapping aus.

HINWEIS: Die Objektdefinitionen für Benutzerkonten, auf welche die Suchkriterien angewendet werden können, sind vordefiniert. Sollten Sie weitere Objektdefinitionen benötigen, um beispielsweise die Vorauswahl der Benutzerkonten weiter einzuschränken, erzeugen Sie im Designer die entsprechenden kundenspezifische Objektdefinitionen. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

- a. Um eine Objektdefinition hinzuzufügen, klicken Sie **Hinzufügen > Kriterium**. Wählen Sie über die Auswahlliste **Anwenden auf** die Objektdefinition aus, für die das Suchkriterium definiert werden soll.

Wenn Sie keine Objektdefinition auswählen, wird das Suchkriterium auf alle Benutzerkonten angewendet.

- b. Um die Objektdefinition eines vorhandenen Suchkriteriums zu ändern, markieren Sie im Bereich **Suchkriterien** das Suchkriterium. Wählen Sie über die Auswahlliste **Anwenden auf** die Objektdefinition aus, für den das Suchkriterium definiert werden soll.

Wenn die bestehende Auswahl entfernt wird, wird das Suchkriterium auf alle Benutzerkonten angewendet.

4. Wählen Sie die Objekteigenschaften für das Mapping aus.
 - **Spalte an Person:** Wählen Sie die Spalte an der Tabelle Person, auf der die Suche ausgeführt wird.
 - **Spalte am Benutzerkonto:** Wählen Sie die Spalte an der Benutzerkonten-Tabelle, die den Wert für die Suche einer Person liefert.
5. Definieren Sie Formatregeln, um das Suchkriterium einzuschränken.

Wählen Sie im Menü **Format hinzufügen** eine Formatvorlage aus. Definieren Sie Formatregeln, die auf die zu suchende Zeichenkette angewendet werden sollen. Es können mehrere Formatvorlagen kombiniert werden.

Tabelle 4: Formatvorlagen

Formatvorlage	Bedeutung
Zeichenbereich	Zeichen der Zeichenkette, die als Suchkriterium genutzt werden sollen.

Formatvorlage	Bedeutung
Beschneide auf feste Länge	Länge der zu suchenden Zeichenkette fest. Damit die feste Länge erreicht wird, kann die Zeichenkette am Beginn oder am Ende mit Füllzeichen ergänzt werden.
Führende oder folgende Zeichen entfernen	Zeichen, die am Anfang oder am Ende der Zeichenkette entfernt werden sollen. Die verbleibende Zeichenkette bildet das Suchkriterium.
Zerteile Wert	Zeichen, bei welchem die Zeichenkette geteilt werden soll und welcher der verbleibenden Teile als Suchkriterium genutzt werden soll.

6. Testen Sie die Formatregeln.

Erfassen Sie im Bereich **Formatierungsvorschau** eine Zeichenkette, auf welche die Formatierung angewendet wird. So können Sie die Auswirkungen Ihrer Formatierung auf das Suchkriterium testen.

7. Wenden Sie die Formatregeln an.

Aktivieren Sie **Formatierung anwenden** an den Spalten, für die das Suchkriterium eingeschränkt werden soll.

8. Speichern Sie die Änderungen.

Für ein Suchkriterium können verschiedene Objekteigenschaften verknüpft werden. Dabei können sowohl UND- als auch ODER-Verknüpfungen realisiert werden.

Beispiel: UND-Verknüpfung

Um Personen an Notes Benutzerkonten zuzuordnen, müssen sowohl der Nachname als auch der Vorname von Person und Benutzerkonto identisch sein. Folgende Tabellenspalten werden gemappt:

UND

Person.Firstname - NotesUser.Firstname

Person.LastName - NotesUser.LastName

Beispiel: ODER-Verknüpfung

Um Personen an Active Directory Benutzerkonten zuzuordnen, müssen entweder das zentrale Benutzerkonto der Person und der Anmeldename des Benutzerkontos

identisch sein oder der vollständige Name der Person und der Anzeigename des Benutzerkontos. Folgende Tabellenspalten werden gemappt:

ODER

Person.CentralAccount - ADSAccount.SAMAccountName

Person.InternalName - ADSAccount.DisplayName

Um Objekteigenschaften für ein Suchkriterium zu verknüpfen

1. Markieren Sie im Bereich **Suchkriterien** den Operator, zu dem eine weitere Objekteigenschaft hinzugefügt werden soll. Klicken Sie **Operator ändern**, um den Operator für die Verknüpfung auszuwählen.
2. Klicken Sie **Hinzufügen > Kriterium**.
3. Wählen Sie die Objekteigenschaften für das Mapping aus.
4. Definieren Sie Formatregeln und wenden Sie diese an.
5. Wenn Sie Verknüpfungen verschachteln wollen, klicken Sie **Hinzufügen > UND-Operator** oder **Hinzufügen > ODER-Operator** und führen Sie die Schritte 2 bis 4 erneut aus.
6. Speichern Sie die Änderungen.

Um ein Suchkriterium zu löschen

1. Markieren Sie das Suchkriterium und klicken Sie **Entfernen**.
2. Speichern Sie die Änderungen.

Personen suchen und direkt an Benutzerkonten zuordnen

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

Tabelle 5: Ansichten zur manuellen Zuordnung

Ansicht	Beschreibung
Vorgeschlagene Zuordnungen	Die Ansicht listet alle Benutzerkonten auf, denen der One Identity Manager eine Person zuordnen kann. Dazu werden die Personen angezeigt, die durch die Suchkriterien ermittelt und zugeordnet werden können.
Zugeordnete Benut-	Die Ansicht listet alle Benutzerkonten auf, denen eine Person

Ansicht	Beschreibung
zerkonten	zugeordnet ist.
Ohne Personenzuordnung	Die Ansicht listet alle Benutzerkonten auf, denen keine Person zugeordnet ist und für die über die Suchkriterien keine passende Person ermittelt werden kann.

Um Suchkriterien auf die Benutzerkonten anzuwenden

- Im unteren Bereich des Formulars **Suchkriterien für die Personenzuordnung definieren** klicken Sie **Neu laden**.

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

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

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

Um Personen direkt über die Vorschlagsliste zuzuordnen

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

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

Um Zuordnungen zu entfernen

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

Anpassen der Skripte für die automatische Personenzuordnung

Die automatische Personenzuordnung wird durch Skripte gesteuert. Diese Skripte ordnen im Modus **SEARCH** anhand der definierten Suchkriterien vorhandene Personen an die Benutzerkonten zu. Darüber hinaus definieren die Skripte für den Modus **CREATE** die Eigenschaften, die bei Erzeugung einer neuen Person initialisiert werden. Diese Skripte sind in einer One Identity Manager Standardinstallation für jeden Zielsystemtyp implementiert. Der Name der Skripte lautet:

`<Zielsystemtyp>_PersonAuto_Mapping_<Kontotyp>`

wobei:

`<Zielsystemtyp>` = Kurzbezeichnung des angesprochenen Zielsystemtyps

`<Kontotyp>` = Tabelle, welche die Benutzerkonten enthält

TIPP: Um die Suchkriterien für die automatische Personenzuordnung oder die Eigenschaften der neu zu erzeugenden Personen zu erweitern, können Sie die Skripte unternehmensspezifisch anpassen. Die Skripte sind überschreibbar. Erstellen Sie dafür eine Kopie eines vorhandenen Skripts und erweitern Sie die Kopie unternehmensspezifisch.

Bei der automatischen Personenzuordnung im Modus **CREATE** werden einige Eigenschaften des Benutzerkontos an das neue Personenobjekt übergeben. Diese Personeneigenschaften werden ebenfalls über die Skripte definiert. Die Initialisierung von Eigenschaften bei der Erzeugung einer Person zu einem Benutzerkonto erfolgt dabei über die Auswertung der Einträge in der Tabelle `DialogNotification`. In dieser Tabelle werden die über Bildungsregeln verbundenen Eigenschaften als Sender-Empfänger-Paar abgebildet. Die Auswertung der Einträge in `DialogNotification` ist nachfolgend beispielhaft für die Initialisierung des Nachnamens einer Person erläutert.

Beispiel:

Der Nachname eines Active Directory Benutzerkontos wird aus dem Nachnamen der Person gebildet.

Bildungsregel auf ADSAccount.Surname:

```
Value = $FK(UID_Person).Lastname$
```

Erfolgt eine Änderung des Nachnamens der Person wird der Nachname des Active Directory Benutzerkontos ebenfalls geändert. Die Spalte Person.Lastname ist somit der Sender und die Spalte ADSAccount.Surname ist der Empfänger.

Beziehung laut Tabelle DialogNotification:

```
Person.Lastname -- > ADSAccount.Surname
```

Die Tabelle DialogNotification kann beim Initialisieren der Eigenschaften einer neuen Person zur Hilfe genommen werden, indem diese Beziehungen rückwärts aufgelöst werden. Der Nachname der Person kann durch den Nachnamen des Active Directory Benutzerkontos bestückt werden. Damit können also bereits einige Vorbesetzungen für das Personenobjekt automatisch generiert werden. Allerdings können nur eindeutige Beziehungen aufgelöst werden.

Beispiel:

Der Anzeigename eines Active Directory Benutzerkontos soll aus dem Nachnamen und dem Vornamen einer Person gebildet werden.

Beziehungen laut Tabelle DialogNotification:

```
Person.Lastname -- > ADSAccount.Displayname
```

```
Person.Firstname -- > ADSAccount.Displayname
```

Hier können Person.Firstname und Person.Lastname nicht aus ADSAccount.Displayname ermittelt werden, da dieser ein zusammengesetzter Wert ist.

Um das Mapping von Benutzerkontoeigenschaften auf Personeneigenschaften zu erleichtern, können Sie das Skript TSB_PersonAuto_GetPropMappings nutzen. Das Skript wertet die Beziehungen von Eigenschaften unter Nutzung der Tabelle DialogNotification aus. Das Skript erzeugt bei Ausführung über den System Debugger einen VB.Net Skriptcode mit den möglichen Zuweisungen. Diesen Code können Sie dann in das jeweilige Skript <Zielsystemtyp>_PersonAuto_Mapping_<Kontotyp> einfügen.

Beispiel: Ausgabe des Skripts TSB_PersonAuto_GetPropMappings

```
' PROPERTY MAPPINGS ADSAccount - Person
' ADSAccount.Initials -- > Person.Initials
' ADSAccount.Locality-- > Person.City
...
Try
    myPers.PutValue("Initials", myAcc.GetValue("Initials").String)
Catch ex As Exception
End Try
Try
    myPers.PutValue("City", myAcc.GetValue("Locality").String)
Catch ex As Exception
End Try
...
```

Deaktivieren und Löschen von Personen und Benutzerkonten

Der Umgang mit Personen, vor allem beim dauerhaften oder zeitweisen Ausscheiden einer Person aus dem Unternehmen, wird in den einzelnen Unternehmen unterschiedlich gehandhabt. Es gibt Unternehmen, die Personen nie löschen, sondern nur deaktivieren, wenn sie das Unternehmen verlassen. Andere Unternehmen wollen Personen löschen, jedoch erst dann, wenn sichergestellt ist, dass alle Benutzerkonten gelöscht wurden. Auch für die Gruppenmitgliedschaften der Benutzerkonten können unterschiedliche Anforderungen gelten.

Wie Benutzerkonten und ihre Gruppenmitgliedschaften behandelt werden, wenn Personen deaktiviert oder gelöscht werden, ist abhängig von der Art der Verwaltung der Benutzerkonten.

Es gelten folgende Szenarien:

- Benutzerkonten sind mit Personen verbunden und werden über Kontendefinitionen verwaltet.
- Benutzerkonten sind mit Personen verbunden. Es sind keine Kontendefinitionen zugeordnet.

Detaillierte Informationen zum Thema

- [Zeitweilige Deaktivierung von Personen](#) auf Seite 34
- [Dauerhafte Deaktivierung von Personen](#) auf Seite 35
- [Verzögertes Löschen von Personen](#) auf Seite 37
- [Deaktivieren und Löschen über Kontendefinitionen](#) auf Seite 38
- [Behandlung von Gruppenmitgliedschaften](#) auf Seite 41

Zeitweilige Deaktivierung von Personen

Die Person ist momentan nicht im Unternehmen, mit der Rückkehr wird zu einem definierten Termin gerechnet. Das gewünschte Verhalten kann sein, dass die Benutzerkonten gesperrt werden und alle Gruppenmitgliedschaften entzogen werden. Oder es sollen die Benutzerkonten gelöscht, bei Wiedereintritt jedoch wieder hergestellt werden, wenn auch mit einer neuen System Identifikationsnummer (SID).

Die zeitweilige Deaktivierung einer Person wird ausgelöst durch:

- die Option **Zeitweilig deaktiviert**
- das Start- und Enddatum der Deaktivierung (**Zeitweilig deaktiviert ab** und **Zeitweilig deaktiviert bis**)

HINWEIS:

- Konfigurieren Sie im Designer den Zeitplan **Benutzerkonten ausgeschiedener Personen sperren**. Dieser Zeitplan prüft das Startdatum der Deaktivierung und setzt bei Erreichen des Startdatums die Option **Zeitweilig deaktiviert**.
- Konfigurieren Sie im Designer den Zeitplan **Zeitweise deaktivierte Benutzerkonten aktivieren**. Dieser Zeitplan überwacht das Enddatum der Deaktivierung und aktiviert bei Ablauf des Datums die Person und ihre Benutzerkonten wieder. Benutzerkonten einer Person, die bereits vor einer zeitweiligen Deaktivierung der Person deaktiviert waren, werden nach Ablauf des Zeitraumes ebenfalls wieder aktiviert.

Szenario: Benutzerkonten sind mit Personen verbunden und werden über Kontendefinitionen verwaltet.

- Legen Sie an den Kontendefinitionen fest, welche Auswirkungen die zeitweilige Deaktivierung von Personen auf die Benutzerkonten haben soll. Für jeden Automatisierungsgrad können Sie über die Option **Benutzerkonten bei zeitweiliger Deaktivierung sperren** festlegen, ob die Benutzerkonten für die Zeit der Deaktivierung gesperrt werden oder aktiviert bleiben.
- Legen Sie an den Kontendefinitionen fest, welche Auswirkungen die zeitweilige Deaktivierung von Personen auf die Gruppenmitgliedschaften der Benutzerkonten haben soll. Für jeden Automatisierungsgrad können Sie über die Option **Gruppen bei zeitweiliger Deaktivierung beibehalten** festlegen, ob beim Deaktivieren von

Personen die Gruppenmitgliedschaften der Benutzerkonten erhalten bleiben oder entfernt werden.

Szenario: Benutzerkonten sind mit Personen verbunden. Es sind keine Kontendefinitionen zugeordnet.

- Legen Sie das gewünschte Verhalten über den Konfigurationsparameter **QER | Person | TemporaryDeactivation** fest. Ist der Konfigurationsparameter aktiviert, werden für die Zeit der Deaktivierung die Benutzerkonten einer Person gesperrt. Ist der Konfigurationsparameter deaktiviert, haben die Eigenschaften der verbundenen Person keinen Einfluss auf die Benutzerkonten.
- Gruppenmitgliedschaften von Benutzerkonten bleiben bestehen. Implementieren Sie bei Bedarf unternehmensspezifische Prozesse, um die Gruppenmitgliedschaften zu entfernen.

Verwandte Themen

- [Dauerhafte Deaktivierung von Personen](#) auf Seite 35
- [Verzögertes Löschen von Personen](#) auf Seite 37
- [Deaktivieren und Löschen über Kontendefinitionen](#) auf Seite 38
- [Behandlung von Gruppenmitgliedschaften](#) auf Seite 41

Dauerhafte Deaktivierung von Personen

Personen können dauerhaft deaktiviert werden, beispielsweise wenn sie aus dem Unternehmen ausscheiden. Dabei kann es erforderlich sein, dass diesen Personen ihre Berechtigungen in den angeschlossenen Zielsystem und ihre Unternehmensressourcen entzogen werden.

Die Auswirkungen der dauerhaften Deaktivierung einer Person sind:

- Die Person kann nicht als Manager an Personen zugewiesen werden.
- Die Person kann nicht als Verantwortlicher an Rollen zugewiesen werden.
- Die Person kann nicht als Eigentümer an Attestierungsrichtlinien zugewiesen werden.
- Es erfolgt keine Vererbung von Unternehmensressourcen über Rollen, wenn zusätzlich die Option **Keine Vererbung** an der Person aktiviert ist.
- Benutzerkonten der Person werden gesperrt oder gelöscht und den Benutzerkonten werden die Gruppenmitgliedschaften entzogen.

Die dauerhafte Deaktivierung einer Person wird ausgelöst über:

- die Aufgabe **Person dauerhaft deaktivieren**

Die Aufgabe sorgt dafür, dass die Option **Dauerhaft deaktiviert** aktiviert wird und das Austrittsdatum und das Datum des letzten Arbeitstages auf den aktuellen Tag gesetzt werden.

- das Erreichen des Austrittsdatums

HINWEIS:

- Prüfen Sie im Designer den Zeitplan **Benutzerkonten ausgeschiedener Personen sperren**. Dieser Zeitplan prüft das Austrittsdatum und setzt bei Erreichen des Austrittsdatums die Option **Dauerhaft deaktiviert**.
- Die Aufgabe **Person erneut aktivieren** sorgt dafür, dass die Person wieder aktiviert wird.

- den Zertifizierungsstatus **Abgelehnt**

Wenn der Zertifizierungsstatus einer Person durch Attestierung oder manuell auf **Abgelehnt** gesetzt wird, wird die Person sofort dauerhaft deaktiviert. Wird der Zertifizierungsstatus auf **Zertifiziert** geändert, wird die Person wieder aktiviert.

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

Szenario: Benutzerkonten sind mit Personen verbunden und werden über Kontendefinitionen verwaltet.

- Legen Sie an den Kontendefinitionen fest, welche Auswirkungen die dauerhafte Deaktivierung von Personen auf die Benutzerkonten haben soll. Für jeden Automatisierungsgrad können Sie über die Option **Benutzerkonten bei dauerhafter Deaktivierung sperren** festlegen, ob die Benutzerkonten für die Zeit der Deaktivierung gesperrt werden oder aktiviert bleiben.
- Legen Sie an den Kontendefinitionen fest, welche Auswirkungen die dauerhafte Deaktivierung von Personen auf die Gruppenmitgliedschaften der Benutzerkonten haben soll. Für jeden Automatisierungsgrad können Sie über die Option **Gruppen bei dauerhafter Deaktivierung beibehalten** festlegen, ob beim Löschen einer Person die Gruppenmitgliedschaften der Benutzerkonten erhalten bleiben oder entfernt werden.

Szenario: Benutzerkonten sind mit Personen verbunden. Es sind keine Kontendefinitionen zugeordnet.

- Legen Sie das gewünschte Verhalten über den Konfigurationsparameter **QER | Person | TemporaryDeactivation** fest. Ist der Konfigurationsparameter aktiviert, werden für die Zeit der Deaktivierung die Benutzerkonten der Person gesperrt. Ist der Konfigurationsparameter deaktiviert, haben die Eigenschaften der verbundenen Person keinen Einfluss auf die Benutzerkonten.
- Gruppenmitgliedschaften von Benutzerkonten bleiben bestehen. Implementieren Sie bei Bedarf unternehmensspezifische Prozesse, um die Gruppenmitgliedschaften zu entfernen.

Verwandte Themen

- [Zeitweilige Deaktivierung von Personen](#) auf Seite 34
- [Verzögertes Löschen von Personen](#) auf Seite 37
- [Deaktivieren und Löschen über Kontendefinitionen](#) auf Seite 38
- [Behandlung von Gruppenmitgliedschaften](#) auf Seite 41

Verzögertes Löschen von Personen

Beim Löschen einer Person wird geprüft, ob der Person noch Benutzerkonten und Unternehmensressourcen zugeordnet sind oder ob Bestellungen im IT Shop offen sind. Die Person wird zum Löschen markiert und somit für jede weitere Bearbeitung gesperrt.

Standardmäßig werden Personen mit einer Löschverzögerung von 30 Tagen endgültig aus der Datenbank entfernt. Während dieser Zeit besteht die Möglichkeit die Person wieder zu aktivieren. Nach Ablauf der Löschverzögerung ist ein Wiederherstellen nicht mehr möglich.

Bevor eine Person endgültig aus der One Identity Manager Datenbank gelöscht werden kann, müssen sämtliche Zuweisungen von Unternehmensressourcen entfernt und Bestellungen abgeschlossen werden. Führen Sie diese Aufgabe manuell durch oder implementieren Sie unternehmensspezifische Prozesse.

Alle mit einer Person verbundenen Benutzerkonten können unter bestimmten Voraussetzung standardmäßig durch den One Identity Manager gelöscht werden, sobald eine Person gelöscht wird. Wenn der Person keine weiteren Unternehmensressourcen zugewiesen sind, wird danach auch die Person endgültig gelöscht.

Szenario: Benutzerkonten sind mit Personen verbunden und werden über Kontendefinitionen verwaltet.

- Legen Sie an den Kontendefinitionen fest, welche Auswirkungen das Löschen von Personen auf die Benutzerkonten haben soll. Für jeden Automatisierungsgrad können Sie über die Option **Benutzerkonten bei verzögertem Löschen sperren** festlegen, ob die Benutzerkonten für die Zeit der Löschverzögerung gesperrt werden oder aktiviert bleiben. In jedem Fall werden die Benutzerkonten nach Ablauf der Löschverzögerung aus der One Identity Manager-Datenbank gelöscht.
- Legen Sie an den Kontendefinitionen fest, welche Auswirkungen das Löschen von Personen auf die Gruppenmitgliedschaften der Benutzerkonten haben soll. Für jeden Automatisierungsgrad können Sie über die Option **Gruppen bei verzögertem Löschen beibehalten** festlegen, ob beim Löschen einer Person die Gruppenmitgliedschaften der Benutzerkonten erhalten bleiben oder entfernt werden.

Szenario: Benutzerkonten sind mit Personen verbunden. Es sind keine Kontendefinitionen zugeordnet.

- Implementieren Sie unternehmensspezifische Prozesse, um die verbundenen Benutzerkonten zu löschen. Eine Person bleibt solange zum Löschen markiert, bis sämtliche Benutzerkonten gelöscht und die Zuweisungen übriger Unternehmensressourcen entfernt wurden. Die Benutzerkonten bleiben beim verzögerten Löschen aktiviert bis sie physisch gelöscht werden.
- Legen Sie über den Konfigurationsparameter **QER | Person | User | KeepMembershipsOfLinkedAccount** fest, wie die Gruppenmitgliedschaften der Benutzerkonten behandelt werden. Zulässige Werte sind:
 - **NONE**: Alle Mitgliedschaften werden entzogen. Dies ist das Standardverhalten.
 - **ALL**: Alle Mitgliedschaften bleiben erhalten.
 - **DIRECT**: Direkte Mitgliedschaften bleiben erhalten, vererbte Mitgliedschaften werden entzogen.

WICHTIG: Wenn für eine Gruppe eine Sonderbehandlung für die Vererbung definiert ist, dann werden die Einstellungen des Konfigurationsparameters unter Umständen überschrieben.

Verwandte Themen

- [Zeitweilige Deaktivierung von Personen](#) auf Seite 34
- [Dauerhafte Deaktivierung von Personen](#) auf Seite 35
- [Deaktivieren und Löschen über Kontendefinitionen](#) auf Seite 38
- [Behandlung von Gruppenmitgliedschaften](#) auf Seite 41

Deaktivieren und Löschen über Kontendefinitionen

Werden die Benutzerkonten über Kontendefinitionen verwaltet, dann können Sie das gewünschte Verhalten für die Behandlung der Benutzerkonten und Gruppenmitgliedschaften bei zeitweiliger Deaktivierung, dauerhafter Deaktivierung, Löschen und Sicherheitsgefährdung von Personen über die Kontendefinitionen und Automatisierungsgrade festlegen.

Durch den Zusammenhang eines Zielsystems mit einer Kontendefinition können Sie für jedes Zielsystem eines Zielsystemtyps eine gesonderte Behandlung definieren. Weitere Informationen finden Sie unter [Verwenden von Kontendefinitionen zum Erzeugen von Benutzerkonten](#) auf Seite 10.

Zuweisung von Kontendefinitionen an Personen

Für jede Kontendefinition wird festgelegt, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf

Zuweisung der Kontendefinition selbst auswirken soll. Die Einstellungen eventueller Vorgängerkontendefinitionen werden dabei überschrieben.

Die Zuweisung von Kontendefinitionen an deaktivierte Personen kann beispielsweise gewünscht sein, um bei späterer Aktivierung der Person sicherzustellen, dass sofort alle erforderlichen Berechtigungen ohne Zeitverlust zur Verfügung stehen.

WICHTIG: Solange eine Kontendefinition für eine Person wirksam ist, behält die Person ihre verbundenen Benutzerkonten. Wird die Zuweisung einer Kontendefinition nicht mehr wirksam, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht.

Zur Abbildung des Verhaltens stehen an einer Kontendefinition die folgenden Optionen zur Verfügung.

Tabelle 6: Stammdaten einer Kontendefinition zum Zuweisungsverhalten der Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition bei dauerhafter Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei zeitweiliger Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei verzögertem Löschen beibehalten	Angabe zur Zuweisung der Kontendefinition bei verzögertem Löschen von Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei Sicherheitsgefährdung beibehalten	Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition

Eigenschaft**Beschreibung**

ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.

Behandlung von Benutzerkonten von Personen

Für jeden Automatisierungsgrad wird festgelegt, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten auswirken soll.

Um bei Deaktivierung oder Löschen einer Person die Berechtigungen zu entziehen, können die Benutzerkonten der Person gesperrt werden. Wird die Person zu einem späteren Zeitpunkt wieder aktiviert, werden ihre Benutzerkonten ebenfalls wieder freigeschaltet.

Zur Behandlung der Benutzerkonten sind an einer Kontendefinition für jeden Automatisierungsgrad die folgenden Optionen verfügbar.

Tabelle 7: Stammdaten eines Automatisierungsgrades zur Behandlung von Benutzerkonten

Eigenschaft	Beschreibung
Benutzerkonten bei zeitweiliger Deaktivierung sperren	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Personen gesperrt werden sollen.
Benutzerkonten bei dauerhafter Deaktivierung sperren	Gibt an, ob die Benutzerkonten dauerhaft deaktivierter Personen gesperrt werden sollen.
Benutzerkonten bei verzögertem Löschen sperren	Gibt an, ob die Benutzerkonten zum Löschen markierter Personen gesperrt werden sollen.
Benutzerkonten bei Sicherheitsgefährdung sperren	Gibt an, ob die Benutzerkonten von sicherheitsgefährdenden Personen gesperrt werden sollen.

Vererbung von Gruppenmitgliedschaften an die Benutzerkonten der Personen

Für jeden Automatisierungsgrad wird festgelegt, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf die Gruppenmitgliedschaften der Benutzerkonten auswirken soll.

Ist eine Person deaktiviert oder zum Löschen markiert, so können Sie für das Zielsystem einer Kontendefinition die Vererbung der Gruppenmitgliedschaften unterbinden. Dieses Verhalten kann gewünscht sein, wenn die Benutzerkonten und Postfächer einer Person gesperrt sind und somit auch nicht in Verteilerlisten Mitglied sein dürfen. Während der Zeit der Deaktivierung sollten keine Vererbungsvorgänge für diese Personen berechnet werden. Bestehende Gruppenmitgliedschaften werden gelöscht.

Zur Behandlung der Gruppenmitgliedschaften sind an einer Kontendefinition für jeden Automatisierungsgrad die folgenden Optionen verfügbar.

Tabelle 8: Stammdaten einer Automatisierungsgrades zur Behandlung von Gruppenmitgliedschaften

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

HINWEIS: Die Vererbungseinstellungen können für einzelne Gruppen überschrieben werden. Weitere Informationen finden Sie unter [Behandlung von Gruppenmitgliedschaften](#) auf Seite 41.

Verwandte Themen

- [Zeitweilige Deaktivierung von Personen](#) auf Seite 34
- [Dauerhafte Deaktivierung von Personen](#) auf Seite 35
- [Verzögertes Löschen von Personen](#) auf Seite 37

Behandlung von Gruppenmitgliedschaften

Die Behandlung von Gruppenmitgliedschaften beim Deaktivieren oder Löschen von Benutzerkonten ist abhängig von der Art der Verwaltung der Benutzerkonten.

Szenario: Benutzerkonten sind mit Personen verbunden und werden über Kontendefinitionen verwaltet.

- Über die Automatisierungsgrade der Kontendefinitionen legen Sie fest, wie Gruppenmitgliedschaften von Benutzerkonten bei der zeitweiligen Deaktivierung, bei der dauerhaften Deaktivierung, beim Löschen und bei Sicherheitsgefährdung von Personen behandelt werden sollen.

Szenario: Benutzerkonten sind mit Personen verbunden. Es sind keine Kontendefinitionen zugeordnet.

- Wird eine Person zeitweilig oder dauerhaft deaktiviert, bleiben die Gruppenmitgliedschaften der Benutzerkonten erhalten.
- Für das verzögerte Löschen kann das Verhalten über den Konfigurationsparameter **QER | Person | User | KeepMembershipsOfLinkedAccount** festgelegt werden.

Vererbungseinstellungen für einzelne Gruppen überschreiben

Unter Umständen kann es erforderlich sein, für einzelne Gruppen ein abweichendes Verhalten zu definieren. Es kann beispielsweise definiert werden, dass eine Gruppe niemals automatisch von Benutzerkonten entfernt werden soll oder die Einstellungen der Kontendefinition überschrieben werden.

Für Gruppen können Sie für folgende Vererbungseinstellungen ein vom Standard abweichendes Verhalten festlegen.

- Gruppen bei zeitweiliger Deaktivierung beibehalten
- Gruppen bei dauerhafter Deaktivierung beibehalten
- Gruppen bei verzögertem Löschen beibehalten
- Gruppen bei Sicherheitsgefährdung beibehalten
- Gruppen bei deaktiviertem Benutzerkonto beibehalten

Zulässige Werte sind:

- **Laut Automatisierungsgrad:** Für die Gruppenmitgliedschaften gelten die Einstellungen des Automatisierungsgrades. Über die Automatisierungsgrade der Kontendefinitionen legen Sie fest, wie Gruppenmitgliedschaften bei der zeitweiligen Deaktivierung, bei der dauerhaften Deaktivierung, beim Löschen und bei Sicherheitsgefährdung von Personen behandelt werden sollen.

Die Einstellung ist wirksam für Benutzerkonten, die mit Personen verbunden sind und über Kontendefinitionen verwaltet werden.

- **Niemals:** Die Gruppe wird niemals vererbt. Bestehende Gruppenmitgliedschaften werden entfernt. Die Zuweisung der Gruppen bleibt erhalten, diese Zuweisung wird jedoch nicht wirksam.

Die Einstellung ist wirksam für Benutzerkonten, die mit Personen verbunden sind. Die Einstellung wirkt unabhängig davon, ob die Benutzerkonten über Kontendefinitionen verwaltet werden oder nicht.

WICHTIG: Wird für die Einstellung **Gruppen bei deaktiviertem Benutzerkonto beibehalten** der Wert **Niemals** verwendet, werden auch die Gruppenmitgliedschaften von Benutzerkonten unwirksam, die nicht mit einer Person verbunden sind.



HINWEIS: Die Einstellungen des Konfigurationsparameters **QER | Person | User | KeepMembershipsOfLinkedAccount** werden überschrieben.

- **Immer:** Die Gruppe wird immer vererbt. Bestehende Gruppenmitgliedschaften bleiben erhalten.

Die Einstellung ist wirksam für Benutzerkonten, die mit Personen verbunden sind. Die Einstellung wirkt unabhängig davon, ob die Benutzerkonten über Kontendefinitionen verwaltet werden oder nicht.

HINWEIS: Die Einstellungen des Konfigurationsparameters **QER | Person | User | KeepMembershipsOfLinkedAccount** werden überschrieben.

Um die Vererbungseinstellungen zu überschreiben

1. Wählen Sie im Manager die Kategorie **<Zielsystemtyp> > Gruppen > Vererbungseinstellungen überschreiben**.
2. Um eine neue Gruppe aufzunehmen, klicken Sie in der Ergebnisliste .
 - a. Klicken Sie neben dem Eingabefeld **Gruppe** auf die Schaltfläche  .
 - b. Wählen Sie unter **Tabelle** die Tabelle, welche die Gruppe abbildet.
 - c. Wählen Sie unter **Gruppe** die Gruppe.
 - d. Klicken Sie **OK**.
- ODER -
3. Um die Werte für eine bestehende Gruppe zu ändern, wählen Sie in der Ergebnisliste die Gruppe.
4. Erfassen Sie die Werte für die Vererbungseinstellungen.
5. Speichern Sie die Änderungen.

HINWEIS: Abhängig vom Zielsystemtyp können die Vererbungseinstellungen für weitere Arten von Berechtigungen überschrieben werden.

Verwandte Themen

- [Zeitweilige Deaktivierung von Personen](#) auf Seite 34
- [Dauerhafte Deaktivierung von Personen](#) auf Seite 35
- [Deaktivieren und Löschen über Kontendefinitionen](#) auf Seite 38
- [Verzögertes Löschen von Personen](#) auf Seite 37

Der Unified Namespace

Der Unified Namespace ist ein virtuelles System, in dem die unterschiedlichsten Zielsysteme mit ihren Strukturen, Benutzerkonten, Systemberechtigungen und Mitgliedschaften abgebildet werden. Durch den Unified Namespace wird eine allgemeine, zielsystemübergreifende Abbildung aller angeschlossenen Zielsysteme erreicht. Dabei können Zielsysteme wie beispielsweise Active Directory Domänen ebenso abgebildet werden wie kundendefinierte Zielsysteme.

Durch die Abbildung der Zielsysteme im Unified Namespace können Sie weitere Kernfunktionen des One Identity Manager, wie das Identity Audit, die Attestierung oder die Berichtsfunktion, zielsystemübergreifend nutzen. Verschiedene Berichte werden standardmäßig mitgeliefert.

Detaillierte Informationen zum Thema

- [Abbildung der Zielsystemobjekte im Unified Namespace](#) auf Seite 44
- [Besonderheiten bei der Abbildung von Objekteigenschaften](#) auf Seite 50
- [One Identity Manager Benutzer für die Verwaltung von Zielsystemen im Unified Namespace](#) auf Seite 51
- [Unified Namespace Objekte anzeigen](#) auf Seite 52
- [Berichte über ein Zielsystem im Unified Namespace](#) auf Seite 52
- [Berichte über alle Zielsysteme im Unified Namespace](#) auf Seite 56

Abbildung der Zielsystemobjekte im Unified Namespace

Jeder Objekttyp des Unified Namespace vereinigt verschiedene Tabellen des One Identity Manager Schemas, in denen die Objekte der angeschlossenen Zielsysteme abgebildet sind. Die verschiedenen Zielsystemtabellen werden in Datenbanksichten vereinigt. Dadurch können die unterschiedlichen Objekteigenschaften einheitlich abgebildet werden.

Um Complianceprüfungen oder Attestierungen zielsystemübergreifend durchzuführen und um zielsystemübergreifende Berichte zu erstellen, nutzen Sie die folgenden Datenbanksichten.

Zielsysteme (UNSRoot)

Die Sicht UNSRoot bildet die Basisobjekte der Synchronisation der Zielsysteme ab.

Zielsystemtyp	Tabelle
Active Directory	ADSDomain
Microsoft Exchange	EX0Organization
SharePoint	SPSSite
SharePoint Online	O3SSite
HCL Domino	NotesDomain
SAP R/3	SAPMandant
LDAP	LDPDomain
Kundendefinierte Zielsysteme	UNSRootB
Unix	UNXHost
Azure Active Directory	AADOrganization
Google Workspace	GAPCustomer
Cloud Zielsysteme	CSMRoot
Oracle E-Business Suite	EBSSystem
Privileged Account Management	PAGAppliance

Container (UNSContainer)

Die Sicht UNSContainer bildet die Containerstrukturen der Zielsysteme ab.

Zielsystemtyp	Tabelle
Active Directory	ADSContainer
SharePoint	SPSWeb
SharePoint Online	O3SWeb
LDAP	LDAPContainer
Kundendefinierte Zielsysteme	UNSContainerB
Cloud Zielsysteme	CSMContainer
Google Workspace	GAPOrgUnit

Benutzerkonten (UNSAccount)

Die Sicht UNSAccount bildet die Benutzerkonten der Zielsysteme ab.

Zielsystemtyp	Tabelle
Active Directory	ADSAccount, ADSContact
Microsoft Exchange	EX0MailUser, EX0MailContact, EX0Mailbox
SharePoint	SPSUser
SharePoint Online	O3SUser
HCL Domino	NotesUser
SAP R/3	SAPUser, SAPBWUser, SAPUserMandant
LDAP	LDAPAccount
Kundendefinierte Zielsysteme	UNSAccountB
Unix	UNXAccount
Azure Active Directory	AADUser
Exchange Online	O3EMailbox, O3EMailContact, O3EMailUser
Google Workspace	GAPUser
Cloud Zielsysteme	CSMUser
Oracle E-Business Suite	EBSUser
Privileged Account Management	PAGUser

Systemberechtigungen (UNSGroup)

Die Sicht UNSGroup bildet die Systemberechtigungen der Zielsysteme ab, wie beispielsweise Gruppen, Rollen, Profile.

Zielsystemtyp	Tabelle
Active Directory	ADSGroup
Microsoft Exchange	EX0DL
SharePoint	SPSGroup, SPSRLAsgn
SharePoint Online	O3SGroup, O3SRLAsgn
HCL Domino	NotesGroup
SAP R/3	SAPGrp, SAPProfile, SAPRole, SAPHRP, SAPBWP
LDAP	LDAPGroup
Kundendefinierte	UNSGroupB, UNSGroupB1, UNSGroupB2, UNSGroupB3

Zielsystemtyp	Tabelle
Zielsysteme	
Unix	UNIXGroup
Azure Active Directory	AADGroup, AADDeniedServicePlan, AADDirectoryRole, AADSubSku
Exchange Online	O3EDL, O3EUnifiedGroup
Google Workspace	GAPGroup, GAPPaSku, GAPOrgAdminRole
Cloud Zielsysteme	CSMGroup, CSMGroup1, CSMGroup2, CSMGroup3
Oracle E-Business Suite	EBSResp
Privileged Account Management	PAGUsrGroup

Berechtigungselemente (UNSIItem)

Die Sicht UNSIItem bildet zusätzliche Berechtigungselemente der Zielsysteme ab.

Zielsystemtyp	Tabelle
Kundendefinierte Zielsysteme	UNSIItemB
Cloud Zielsysteme	CSMItem

Zuweisungen Systemberechtigungen (UNSAccountInUNSGroup)

Die Sicht UNSAccountInUNSGroup bildet die Zuweisungen von Systemberechtigungen an Benutzerkonten der Zielsysteme ab.

Zielsystemtyp	Tabelle
Active Directory	ADSAccountInADSGroup, ADSContactInADSGroup
SharePoint	SPSUserInSPSGroup, SPSUserHASSPSRLAsgn
HCL Domino	NotesUserInGroup
SAP R/3	SAPUserInSAPGrp, HelperSAPUserInSAPRole, SAPUserInSAPProfile, HelperSAPUserInSAPHRP, SAPBWUserInSAPBWP
LDAP	LDAPAccountInLDAPGroup
Kundendefinierte Zielsysteme	UNSAccounBInUNSGroupB, UNSAccounBInUNSGroupB1, UNSAccounBInUNSGroupB2, UNSAccounBInUNSGroupB3, UNSAccounBHasUNSGroupB, UNSAccounBHasUNSGroupB1, UNSAccounBHasUNSGroupB2, UNSAccounBHasUNSGroupB3
Unix	UNXAccountInUNIXGroup

Zielsystemtyp	Tabelle
Azure Active Directory	AADUserHasDeniedService, AADUserInDirectoryRole, AADUserInAADGroup
Exchange Online	O3EAADUserInUnifiedGroup, O3EMailboxInDL, O3EMailContactInDL, O3EMailUserInDL
Google Workspace	GAPUserInGroup, GAPUserInPaSku, GAPUserInOrgAdminRole
Cloud Zielsysteme	CSMUserInGroup, CSMUserInGroup1, CSMUserInGroup2, CSMUserInGroup3, CSMUserHasGroup, CSMUserHasGroup1, CSMUserHasGroup2, CSMUserHasGroup3
Oracle E-Business Suite	EBSUserInRespCompressed
Privileged Account Management	PAGUserInUsrGroup

Zuweisungen Berechtigungselemente (UNSAccountHasUNSIItem)

Die Sicht UNSAccountHasUNSIItem bildet die Zuweisungen zusätzlicher Berechtigungselemente zu den Benutzerkonten der Zielsysteme ab.

Zielsystemtyp	Tabelle
Kundendefinierte Zielsysteme	UNSAccountBHasUNSIItemB
Cloud Zielsysteme	CSMUserHasItem

Zuweisungen Systemberechtigungen (UNSGroupInUNSGroup)

Die Sicht UNSGroupInUNSGroup bildet die Zuweisungen von Systemberechtigungen an Systemberechtigungen der Zielsysteme ab.

Zielsystemtyp	Tabelle
Active Directory	ADSGroupInADSGroup
SharePoint	SPSGroupHasSPSRLAsgn
HCL Domino	NotesGroupInGroup
SAP R/3	SAPProfileInSAPProfile, SAPRoleInSAPRole, SAPProfileInSAPRole
LDAP	LDAPGroupInLDAPGroup
Kundendefinierte Zielsysteme	UNSGroupBInUNSGroupB, UNSGroupBInUNSGroupB1, UNSGroupBInUNSGroupB2, UNSGroupBInUNSGroupB3
Azure Active Directory	AADGroupInGroup

Zielsystemtyp	Tabelle
Exchange Online	O3EDLInDL
Google Workspace	GAPGroupInGroup
Cloud Zielsysteme	CSMGroupInGroup, CSMGroupInGroup1, CSMGroupInGroup2, CSMGroupInGroup3

Zuweisungen Berechtigungselemente (UNSGroupHasUNSIItem)

Die Sicht UNSGroupHasUNSIItem bildet die Zuweisungen zusätzlicher Berechtigungselemente zu den Systemberechtigungen der Zielsysteme ab.

Zielsystemtyp	Tabelle
Kundendefinierte Zielsysteme	UNSGroupBHasUNSIItemB
Cloud Zielsysteme	CSMGroupHasItem

Vererbungsausschluss (UNSGroupExclusion)

Die Sicht UNSGroupExclusion bildet die Definition von Systemberechtigungen ab, die einander ausschließen.

Zielsystemtyp	Tabelle
Active Directory	ADSGroupExclusion
SharePoint	SPSGroupExclusion, SPSRLAsgnExclusion
HCL Domino	NotesGroupExclusion
SAP R/3	SAPGrpExclusion, SAPProfileExclusion, SAPRoleExclusion
LDAP	LDAPGroupExclusion
Kundendefinierte Zielsysteme	UNSGroupBExclusion, UNSGroupB1Exclusion, UNSGroupB2Exclusion, UNSGroupB3Exclusion
Unix	UNIXGroupExclusion
Azure Active Directory	AADGroupExclusion, AADSubSkuExclusion
Google Workspace	GAPGroupExclusion
Cloud Zielsysteme	CSMGroupExclusion, CSMGroup1Exclusion, CSMGroup2Exclusion, CSMGroup3Exclusion
Oracle E-Business Suite	EBSRespExclusion
Privileged Account Management	PAGUsrGroupExclusion

Hierarchie der Systemberechtigungen (UNSGroupCollection)

Die Sicht UNSGroupCollection bildet Hierarchien von Systemberechtigungen ab.

Zielsystemtyp	Tabelle
Active Directory	ADSGroupCollection
SharePoint	SPSGroupCollection, SPSRLAsgn
HCL Domino	NotesGroupCollection
SAP R/3	SAPCollectionRPG
LDAP	LDAPGroupCollection
Kundendefinierte Zielsysteme	UNSGroupBCollection, UNSGroupB1Collection, UNSGroupB2Collection, UNSGroupB3Collection
Unix-basierte Zielsysteme	UNXGroupExclusion
Azure Active Directory	AADGroupCollection
Exchange Online	O3EDLCollection
Google Workspace	GAPGroupCollection
Cloud Zielsysteme	CSMGroupCollection, CSMGroup1Collection, CSMGroup2Collection, CSMGroup3Collection

Besonderheiten bei der Abbildung von Objekteigenschaften

In manchen Zielsystemen können die Zuweisungen von Systemberechtigungen an Benutzerkonten zeitlich befristet sein.

- Im Unified Namespace wird der Gültigkeitszeitraum nicht abgebildet.
- Die Kennzeichnung **Zum Löschen markiert** (UNSAccountInUNSGroup.XMarkedForDeletion) kann für diese Zuweisungen nicht gesetzt werden. Damit ist im Unified Namespace nicht erkennbar, ob eine Zuweisung bei der Synchronisation als ausstehend markiert wurde.

One Identity Manager Benutzer für die Verwaltung von Zielsystemen im Unified Namespace

In die Verwaltung von Zielsystemen im Unified Namespace sind folgende Benutzer eingebunden.

Tabelle 9: Benutzer

Benutzer	Aufgaben
Zielsystemadministratoren	<p>Die Zielsystemadministratoren müssen der Anwendungsrolle Zielsysteme Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen.• Legen die Zielsystemverantwortlichen fest.• Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein.• Legen fest, welche Anwendungsrollen für Zielsystemverantwortliche sich ausschließen.• Berechtigen weitere Personen als Zielsystemadministratoren.• Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.
Zielsystemverantwortliche	<p>Die Zielsystemverantwortlichen müssen der Anwendungsrolle Zielsysteme Unified Namespace oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Erhalten eine zielsystemübergreifende Sicht auf die Objekte der angeschlossenen Zielsysteme.• Können zielsystemübergreifende Berichte erstellen. <p>Sind die Benutzer gleichzeitig Zielsystemverantwortliche der zugrunde liegenden Zielsysteme, können sie diese Zielsysteme über den Unified Namespace verwalten.</p>
One Identity Manager Administratoren	<p>One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen.</p>

One Identity Manager Administratoren:

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

Unified Namespace Objekte anzeigen

HINWEIS: Die Objekteigenschaften und Zuweisungen können im Unified Namespace nicht bearbeitet werden. Verwenden Sie die Aufgabe **Basisobjekt anzeigen** um zum verbundenen Zielsystemobjekt zu wechseln. Als Zielsystemadministrator können Sie die Objekte Ihres Zielsystems wie gewohnt bearbeiten.

Um die Objekte des Unified Namespace anzuzeigen

- Wählen Sie im Manager die Kategorie **Unified Namespace**.

In der Navigationsansicht werden die Benutzerkonten, Systemberechtigungen und Strukturelemente aller angebotenen Zielsysteme hierarchisch dargestellt. Es können die Stammdaten und existierenden Zuweisungen aller Objekte angezeigt werden. Die Objekteigenschaften und Zuweisungen können nicht bearbeitet werden.

Berichte über ein Zielsystem im Unified Namespace

Der One Identity Manager stellt verschiedene Berichte zur Verfügung mit Informationen über ein Zielsystem, das im Unified Namespace abgebildet ist.

Tabelle 10: Berichte zur Datenqualität eines Zielsystems

Bericht	Bereitgestellt für	Beschreibung
Übersicht anzeigen	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Herkunft)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die Herkunft der zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Historie)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (Min. Datum). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Benutzerkonten anzeigen (inklusive Historie)	Container	Der Bericht zeigt alle Benutzerkonten des Containers mit ihren Berechtigungen einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (Min. Datum). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Systemberechtigungen anzeigen (inklusive Historie)	Container	Der Bericht zeigt die Systemberechtigungen des Containers mit den zugewiesenen Benutzerkonten einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (Min. Datum). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Container	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Container mindestens ein Benutzerkonto besitzen.

Bericht	Bereitgestellt für	Beschreibung
Übersicht aller Zuweisungen	Systemberechtigung	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, welche die ausgewählte Systemberechtigung besitzen.
Übersicht anzeigen	Systemberechtigung	Der Bericht zeigt einen Überblick über die Systemberechtigung und ihre Zuweisungen.
Übersicht anzeigen (inklusive Herkunft)	Systemberechtigung	Der Bericht zeigt einen Überblick über die Systemberechtigung und die Herkunft der zugewiesenen Benutzerkonten.
Übersicht anzeigen (inklusive Historie)	Systemberechtigung	Der Bericht zeigt einen Überblick über die Systemberechtigung einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (Min. Datum). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Historische Mitgliedschaften anzeigen	Systemberechtigung	Der Bericht zeigt alle Personen, die einem Benutzerkonto dieser Systemberechtigung zugeordnet sind, einschließlich der Dauer der Mitgliedschaft. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (Min. Datum). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Abweichende Systemberechtigungen anzeigen	Zielsystem	Der Bericht enthält alle Systemberechtigungen, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager.
Benutzerkonten anzeigen (inklusive Historie)	Zielsystem	Der Bericht liefert alle Benutzerkonten mit ihren Berechtigungen einschließlich eines historischen Verlaufs.

Bericht	Bereitgestellt für	Beschreibung
		Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (Min. Datum). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Benutzerkonten mit einer überdurchschnittlichen Anzahl an Systemberechtigungen anzeigen	Zielsystem	Der Bericht enthält alle Benutzerkonten, die eine überdurchschnittliche Anzahl an Systemberechtigungen besitzen.
Personen mit mehreren Benutzerkonten anzeigen	Zielsystem	Der Bericht zeigt alle Personen, die mehrere Benutzerkonten besitzen. Der Bericht enthält eine Risikoeinschätzung.
Systemberechtigungen anzeigen (inklusive Historie)	Zielsystem	Der Bericht zeigt die Systemberechtigungen mit den zugewiesenen Benutzerkonten einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (Min. Datum). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Zielsystem	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Zielsystem mindestens ein Benutzerkonto besitzen.
Ungenutzte Benutzerkonten anzeigen	Zielsystem	Der Bericht enthält alle Benutzerkonten, die in den letzten Monaten nicht verwendet wurden.
Unverbundene Benutzerkonten anzeigen	Zielsystem	Der Bericht zeigt alle Benutzerkonten, denen keine Person zugeordnet ist.
Veränderungen an Benutzerkonten anzeigen	Zielsystem	Der Bericht zeigt für einen bestimmten Zeitraum die geänderten Benutzerkonten aller Zielsysteme an.

Berichte über alle Zielsysteme im Unified Namespace

Der One Identity Manager stellt verschiedene Berichte zur Verfügung mit Informationen über alle Zielsysteme, die im Unified Namespace abgebildet sind. Die Daten werden nach Zielsystemtyp gruppiert und zusammengefasst.

Tabelle 11: Berichte zur Datenqualität aller Zielsysteme

Bericht	Beschreibung
Unverbundene Benutzerkonten aus allen Zielsystemen	Der Bericht zeigt alle Benutzerkonten, denen keine Person zugeordnet ist. Den Bericht finden Sie in der Kategorie Mein One Identity Manager > Übersichten Datenqualität .
Ungenutzte Benutzerkonten aus allen Zielsystemen	Der Bericht enthält alle Benutzerkonten, die in den letzten Monaten nicht verwendet wurden. Den Bericht finden Sie in der Kategorie Mein One Identity Manager > Übersichten Datenqualität .
Abweichende Systemberechtigungen aus allen Zielsystemen	Der Bericht enthält alle Systemberechtigungen, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager. Den Bericht finden Sie in der Kategorie Mein One Identity Manager > Übersichten Datenqualität .
Benutzerkonten mit einer überdurchschnittlichen Anzahl an Systemberechtigungen	Der Bericht enthält alle Benutzerkonten, die eine überdurchschnittliche Anzahl an Systemberechtigungen besitzen. Den Bericht finden Sie in der Kategorie Mein One Identity Manager > Übersichten Datenqualität .
Unified Namespace Benutzerkonten-Systemberechtigungen-Verteilung	Der Bericht zeigt einen Überblick über die Verteilung der Benutzerkonten und Systemberechtigungen im Unified Namespace. Den Bericht finden Sie in der Kategorie Mein One Identity Manager > Übersichten Zielsysteme .
Veränderungen an Benutzerkonten aus allen Zielsystemen	Der Bericht zeigt für einen bestimmten Zeitraum die geänderten Benutzerkonten aller Zielsysteme an. Den Bericht finden Sie in der Kategorie Mein One Identity Manager > Übersichten Zielsysteme .

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

B

Benutzerkonto

- Automatisierungsgrad 7
- befristete Zuweisung 50
- Full managed 7
- Kontendefinition 11
- Linked 7
 - Configured 7
- Person zuordnen (automatisch) 23
- Unlinked 7
- Unmanaged 7
- zentrales 17
- Zustand 7

I

IT Betriebsdaten

- Kontendefinition 11, 13, 15

K

Kontendefinition 10-11, 20

- Automatisierungsgrad 11
- IT Betriebsdaten 11, 13, 15

P

Person

- allgemeine Änderungen 19
- ändern 19
- automatisch zuordnen 23
- dauerhaft deaktivieren 35
- Innerbetrieblicher Wechsel 19

Kontendefinition 11

- löschen 37-38
- Namensänderung 19
- Standard-E-Mail-Adresse 18
- zeitweilig deaktivieren 34
- zentrales Benutzerkonto 17

Personenzuordnung

- automatisch 23
- entfernen 29
- konfigurieren 24
- Kriterium 25
- manuell 29
- Mapping anpassen 31
- Modus"CREATE" 24
- Modus"NO" 24
- Modus"SEARCHE AND CREATE" 24
- Modus"SEARCHE" 24
- Skript anpassen 31
- Suchkriterium 25
 - Formatierung 26
 - Objektyp 26
 - Tabellenspalte 26

S

Suchkriterium

- Personenzuordnung 25

Systemberechtigung

- befristete Zuweisung 50

U

- Unified Namespace 44
 - Berichte 56
 - Objekte
 - Abbildung 44
 - anzeigen 52
 - Zielsystemadministrator 51
 - Zielsystemverantwortlicher 51

Z

- Zuweisung
 - ausstehend 50
 - Gültigkeitszeitraum 50
 - Löschmarkierung 50