One Identity Manager 9.2

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 - 29. September 2023, 05:14 Uhr

Die aktuellsten Versionen der Produktdokumentation finden Sie unter One Identity Manager Dokumentation.

Inhalt

Grundlagen zur Behandlung von Identitäten und Benutzerkonten

Zentraler Bestandteil des One Identity Manager ist die Abbildung von Identitäten 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 Identitäten verbunden werden. Für jede Identität kann damit ein Überblick über ihre Berechtigungen in allen angebundenen Zielsystemen gewonnen werden. Der One Identity Manager bietet die Möglichkeit Benutzerkonten und ihre Berechtigungen zu verwalten. Änderungen können in die Zielsysteme provisioniert werden. Die Identitäten werden so entsprechend ihrer Funktion mit den benötigten Berechtigungen in den angebundenen Zielsystemen versorgt. Regelmäßige Synchronisationsprozesse halten die Daten zwischen den Zielsystemen und der One Identity Manager-Datenbank konsistent.

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

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

Detaillierte Informationen zum Thema

- Administration von Identitäten und Benutzerkonten auf Seite 6
- Behandlung von Identitäten und Benutzerkonten auf Seite 7
- Verwenden von Kontendefinitionen zum Erzeugen von Benutzerkonten auf Seite 11
- Automatische Zuordnung von Identitäten zu Benutzerkonten auf Seite 23
- Deaktivieren und Löschen von Identitäten und Benutzerkonten auf Seite 33

Administration von Identitäten 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 Identität ein Benutzerkonto erzeugt werden. Die Informationen zum Container und Homeserver richten sich nach der Abteilung und dem Standort der Identität. Jedes Benutzerkonto der Domäne erhält automatisch ein Microsoft Exchange Postfach.
- In der Domäne B werden die Benutzerkonten unabhängig von Identitätendaten verwaltet. Microsoft Exchange Postfächer können nur über ein Bestellverfahren vergeben werden.

Zielsystemtyp HCL Domino

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

Zielsystemtyp SAP R/3

- Alle Identitäten der Personalabteilung erhalten automatisch ein Benutzerkonto im SAP Mandanten 101.
- Die Identitäten 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 Identitäten 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 Identitäten erfolgen. Gegebenenfalls können neue Identitäten erzeugt werden und den Benutzerkonten zugeordnet werden. Die Kriterien für diese automatische Zuordnung eines Benutzerkontos zu einer Identität werden unternehmensspezifisch definiert. Nach einer Prüfung der Benutzerkonten kann über Kontendefinitionen der Umfang der Eigenschaften, die eine Identität 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 Identitäten 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 Identität oder durch Zuweisung der Kontendefinition an Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen kann eine Identität über die integrierten Vererbungsmechanismen ein Benutzerkonto erhalten. Kontendefinitionen können automatisch an alle Identitäten 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 Identitäten bei Deaktivierung

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

Behandlung von Identitäten 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 Identitäten verwaltet.
- In der Domäne B werden die Benutzerkonten mit einer Identität verbunden. Es ist jedoch keine Übernahme der Identitätenstammdaten an die Benutzerkonten

erwünscht.

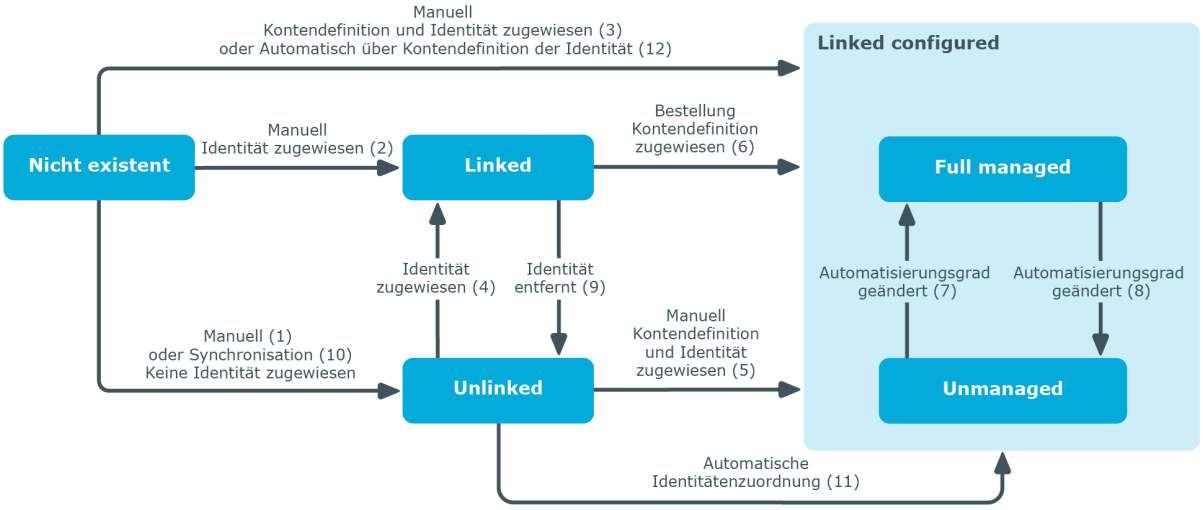
- In der Domäne C soll automatisch für jede interne Identität ein Benutzerkonto erzeugt werden. Die Informationen zum Container, Homeserver und Profilserver richten sich nach der Abteilung und dem Standort der Identität.

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

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

Abbildung 1: Übergangszustände eines Benutzerkontos



Manuelles Einfügen eines Benutzerkontos

- Fall 1: Um ein Benutzerkonto unabhängig von Identitäten zu verwalten, wird das Benutzerkonto manuell angelegt und keine Identität zugewiesen. Das Benutzerkonto ist nicht mit einer Identität verbunden und hat damit den Zustand **Unlinked**.
- Fall 2: Wird das Benutzerkonto bereits beim manuellen Einfügen mit einer Identität verbunden geht das Benutzerkonto in den Zustand **Linked** über.
- Fall 3: Wird beim Anlegen des Benutzerkontos bereits eine Identität 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 Identität zugeordnet, geht das Benutzerkonto aus dem Zustand **Unlinked** in den Zustand **Linked** über.
- Fall 5: Wird einem bestehenden Benutzerkonto manuell eine Identität 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 Identitäten 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 Identität verbunden sind, geändert werden.

Entfernen von Identitätenzuordnungen

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

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

Behandlung der Benutzerkonten bei der Synchronisation

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

Automatische Identitätenzuordnung zu bestehenden Benutzerkonten

- Fall 11: An Benutzerkonten im Zustand **Unlinked** kann der One Identity Manager automatisch Identitäten zuordnen. Wenn dem Zielsystem eine Kontendefinition zugewiesen ist, wird diese Kontendefinition auch an die Identitäten zugewiesen. Abhängig vom verwendeten Automatisierungsgrad wird der Zustand **Linked configured: Unmanaged** oder **Linked configured: Full managed** erreicht. Die automatische Identitätenzuordnung 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 Identitäten zu Benutzerkonten auf Seite 23.

Automatische Erzeugung von Benutzerkonten über Kontendefinitionen

- Fall 12: Um im laufenden Betrieb Benutzerkonten automatisch an Identitäten zu vergeben, werden Kontendefinitionen eingesetzt. Hat eine Identität noch kein Benutzerkonto im Zielsystem, wird durch die Zuweisung der Kontendefinition an eine Identität 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 Identität 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 Identität 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 Identitäten zu vergeben, kennt der One Identity Manager Kontendefinitionen. Kontendefinitionen können für jedes Zielsystem erzeugt werden. Hat eine Identität noch kein Benutzerkonto in einem Zielsystem, wird durch die Zuweisung der Kontendefinition an eine Identität ein neues Benutzerkonto erzeugt.

Aus den Identitätenstammdaten resultieren die Daten für das Benutzerkonto im jeweiligen Zielsystem. Die Identitäten müssen ein zentrales Benutzerkonto besitzen. Über die primäre Zuordnung der Identität 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 Identität 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 Identität 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 Identität. 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 Identität an ihre Benutzerkonten. So kann beispielsweise eine Identität mehrere Benutzerkonten in einem Zielsystem besitzen:

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

One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

- **Unmanaged**: Benutzerkonten mit dem Automatisierungsgrad **Unmanaged** erhalten eine Verbindung zur Identität, erben jedoch keine weiteren Eigenschaften. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Identität werden initial einige der Identitäteneigenschaften übernommen. Werden die Identitäteneigenschaften 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 Identität. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Identität werden initial die Identitäteneigenschaften übernommen. Werden die Identitäteneigenschaften 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 Identität 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 Identität auf Zuweisung der Kontendefinition selbst auswirken soll.

- Solange eine Kontendefinition für eine Identität wirksam ist, behält die Identität ihre verbundenen Benutzerkonten. Die Zuweisung von Kontendefinitionen an deaktivierte Identitäten kann beispielsweise gewünscht sein, um bei späterer Aktivierung der Identität sicherzustellen, das sofort alle erforderlichen Berechtigungen ohne Zeitverlust zur Verfügung stehen.
- Ist die Zuweisung einer Kontendefinition nicht mehr wirksam oder wird die Kontendefinition von der Identität entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht.
- Benutzerkonten, die als **Ausstehend** markiert sind, werden nur gelöscht, wenn der Konfigurationsparameter **QER | Person | User | DeleteOptions | DeleteOutstanding** aktiviert ist.

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

- Um die Berechtigungen zu entziehen, wenn eine Identität deaktiviert, gelöscht oder als sicherheitsgefährdend eingestuft wird, können die Benutzerkonten der Identität gesperrt werden. Wird die Identität 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 Identität gesperrt sind und somit auch nicht in Gruppen Mitglied sein dürfen. Während dieser Zeit sollen keine Vererbungsvorgänge für diese Identitäten berechnet werden. Bestehende Gruppenmitgliedschaften werden dann gelöscht.

Verwandte Themen

- Deaktivieren und Löschen über Kontendefinitionen auf Seite 38

Zuweisen der Kontendefinitionen an Identitäten

Kontendefinitionen werden an die Identitäten des Unternehmens zugewiesen.

Das Standardverfahren für die Zuweisung von Kontendefinitionen an Identitäten ist die indirekte Zuweisung. Die Kontendefinitionen werden an die Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen zugewiesen. Die Identitäten 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 Identitäten zugewiesen werden.

Kontendefinitionen können automatisch an alle Identitäten 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 Identitäten zugewiesen werden oder als Produkte in den IT Shop aufgenommen werden.

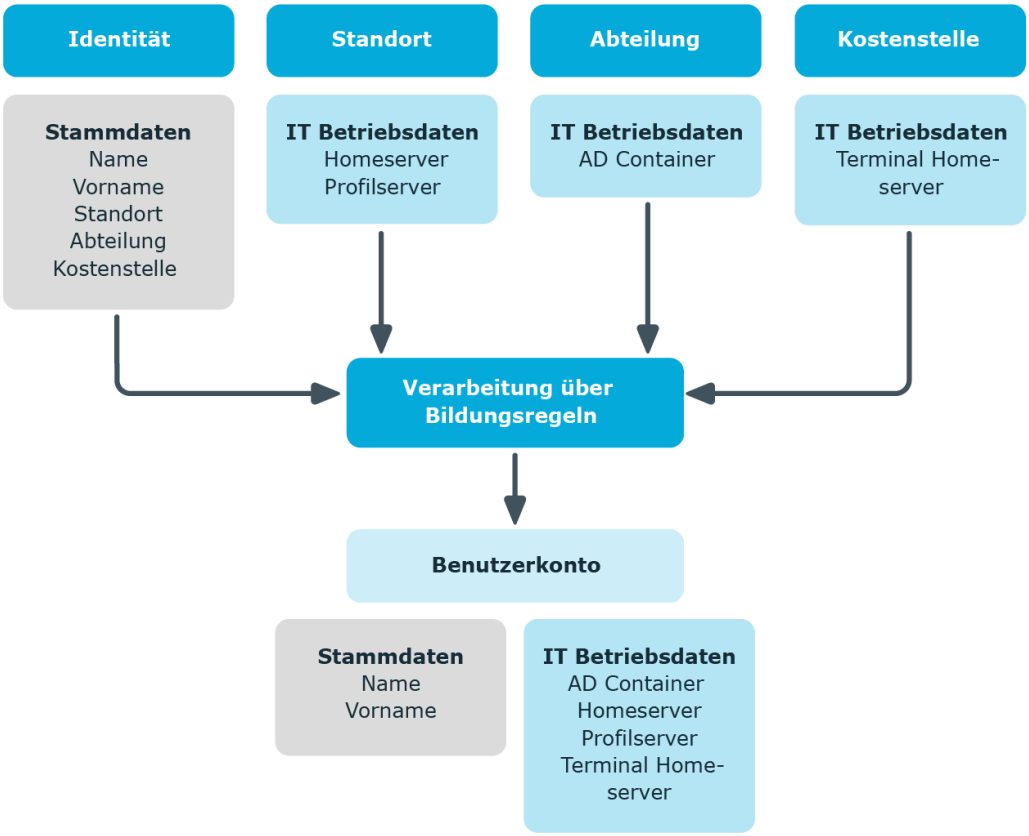
Ermitteln der gültigen IT Betriebsdaten für die Zielsysteme

Um für eine Identität 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 Identität 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 Identität 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 Identität der Abteilung A ein Standardbenutzerkonto in der Domäne A. Zusätzlich erhalten einige Identitäten 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 Identität 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
	Profilserver
	Terminal Homeserver
	Terminal Profilserver
	Gruppen erbbar
	Identitätstyp
	Privilegiertes Benutzerkonto
Microsoft Exchange	Postfachdatenbank
LDAP	Container
	Gruppen erbbar
	Identitätstyp

Zielsystemtyp	IT Betriebsdaten
	Privilegiertes Benutzerkonto
Domino	Server
	Zertifikat
	Vorlage der Postdatei
	Identitätstyp
SharePoint	Authentifizierungsmodus
	Gruppen erbbar
	Rollen erbbar
	Identitätstyp
	Privilegiertes Benutzerkonto
SharePoint Online	Gruppen erbbar
	Rollen erbbar
	Privilegiertes Benutzerkonto
	Authentifizierungsmodus
Kundendefinierte Zielsysteme	Container (je Zielsystem)
	Gruppen erbbar
	Identitätstyp
	Privilegiertes Benutzerkonto
Azure Active Directory	Gruppen erbbar
	Administratorrollen erbbar
	Abonnements erbbar
	Unwirksame Dienstpläne erbbar
	Identitätstyp
	Privilegiertes Benutzerkonto
	Kennwort bei der nächsten Anmeldung ändern
Cloud Zielsystem	Container (je Zielsystem)
	Gruppen erbbar
	Identitätstyp
	Privilegiertes Benutzerkonto
Unix-basierte Zielsysteme	Login-Shell
	Gruppen erbbar

Zielsystemtyp	IT Betriebsdaten
	Identitätstyp
	Privilegiertes Benutzerkonto
Oracle E-Business Suite	Identitätstyp
	Gruppen erbbar
	Privilegiertes Benutzerkonto
SAP R/3	Identitätstyp
	Gruppen erbbar
	Rollen erbbar
	Profile erbbar
	Strukturelle Profile erbbar
	Privilegiertes Benutzerkonto
Exchange Online	Gruppen erbbar
Privileged Account Management	Authentifizierungsanbieter
	Gruppen erbbar
	Identitätstyp
	Privilegiertes Benutzerkonto
Google Workspace	Organisation
	Gruppen erbbar
	Produkte und SKUs erbbar
	Admin-Rollen-Zuordnungen erbbar
	Identitätstyp
	Privilegiertes Benutzerkonto
	Kennwort bei der nächsten Anmeldung ändern
OneLogin	Rollen erbbar
	Identitätstyp
	Privilegiertes Benutzerkonto
	Lizenzierungsstatus
	OneLogin Gruppe

Zentrales Benutzerkonto einer Identität

Das zentrale Benutzerkonto einer Identität 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 One Identity Manager-Standardinstallation wird das zentrale Benutzerkonto aus dem Vornamen und dem Nachnamen der Identität gebildet. Ist nur eine dieser Eigenschaften bekannt, wird diese zur Bildung des zentralen Benutzerkontos genutzt. Es wird in jedem Fall geprüft, 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 2: Beispiel für die Bildung des zentralen Benutzerkontos

Vorname	Nachname	Zentrales Benutzerkonto
Alex		ALEX
	Miller	MILLER
Alex	Miller	ALEXM
Alex	Meyer	ALEXM1

Über den Konfigurationsparameter **QER | Person | CentralAccountGlobalUnique** legen Sie fest, wie das zentrale Benutzerkonto abgebildet wird.

- Ist der Konfigurationsparameter aktiviert, erfolgt die Bildung des zentralen Benutzerkonto einer Identität eindeutig bezogen auf die zentralen Benutzerkonten aller Identitäten und die Benutzerkontennamen aller erlaubten Zielsysteme.
- Ist der Konfigurationsparameter nicht aktiviert, erfolgt die Bildung nur eindeutig bezogen auf die zentralen Benutzerkonten aller Identitäten. Dies ist das Standardverhalten.

Verwandte Themen

- Standard-E-Mail-Adresse einer Identität auf Seite 18
- Ändern von Stammdaten von Identitäten auf Seite 19

Standard-E-Mail-Adresse einer Identität

Die Standard-E-Mail-Adresse der Identität 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 Identität und der Standard-Mail-Domäne der aktivierten Zielsysteme gebildet.

Die Standard-Mail-Domäne wird aus dem Konfigurationsparameter **QER | Person | DefaultMailDomain** ermittelt.

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

Verwandte Themen

- Zentrales Benutzerkonto einer Identität auf Seite 18
- Ändern von Stammdaten von Identitäten auf Seite 19

Ändern von Stammdaten von Identitäten

Nachfolgend wird nur auf die Stammdaten eingegangen, deren Änderungen in der One Identity Manager Standardinstallation Auswirkungen auf die Benutzerkonten einer Identität 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 Identität und ändert die Daten in den Benutzerkonten der Zielsysteme, die der Identität zugeordnet sind, sofern diese Daten im jeweiligen Zielsystem abgebildet sind.

Namensänderung einer Identität

Namensänderungen einer Identität beeinflussen die Bildung des zentralen Benutzerkontos einer Identität. 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 wird. 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 Identität

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 Profilserver, 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 Identität auf Seite 18
- Standard-E-Mail-Adresse einer Identität 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 Identität wird durch die anschließende Skript- und Prozessverarbeitung dafür gesorgt, dass die Identität ihre Benutzerkonten in beiden Zielsystemen erhält.

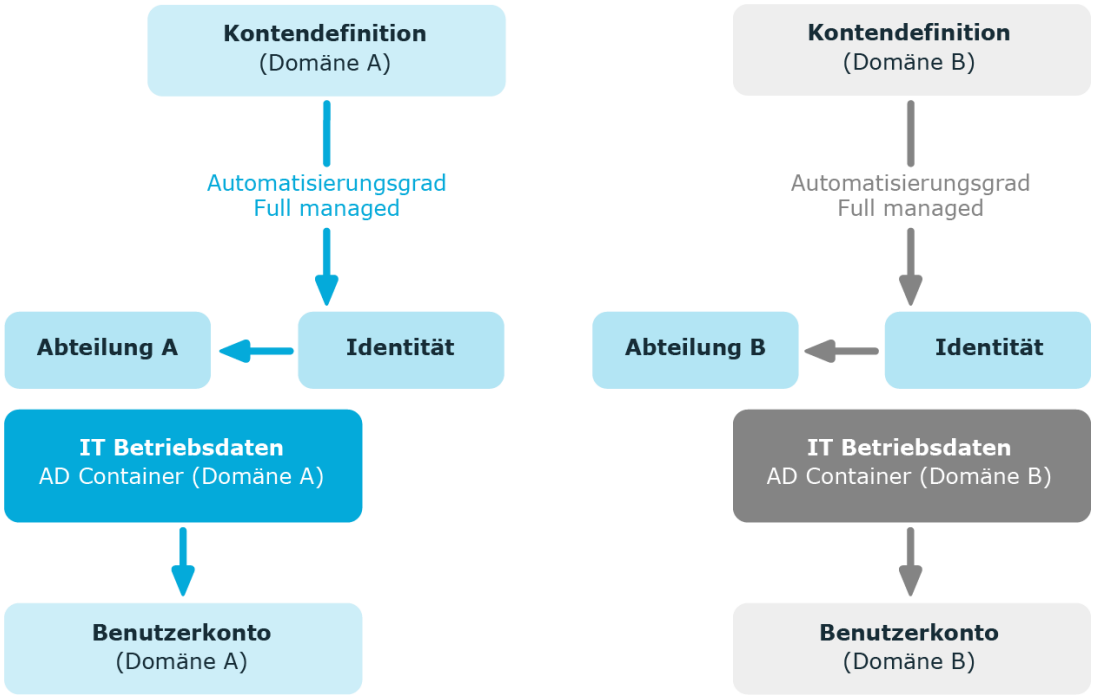
Beispiel: Identitäten können nur in einer Domäne ein Benutzerkonto besitzen

In einer Active Directory-Umgebung existieren zwei Domänen. Die Identitäten können nur in einer der beiden Domänen ein Benutzerkonto besitzen. Anhand der IT Betriebsdaten der Abteilung einer Identität 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 Identität zur Abteilung A, dann erhält Sie, beispielsweise per dynamischer Zuweisung, die Kontendefinition A und daraus resultierend ein Benutzerkonto in Domäne A. Gehört die Identität 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

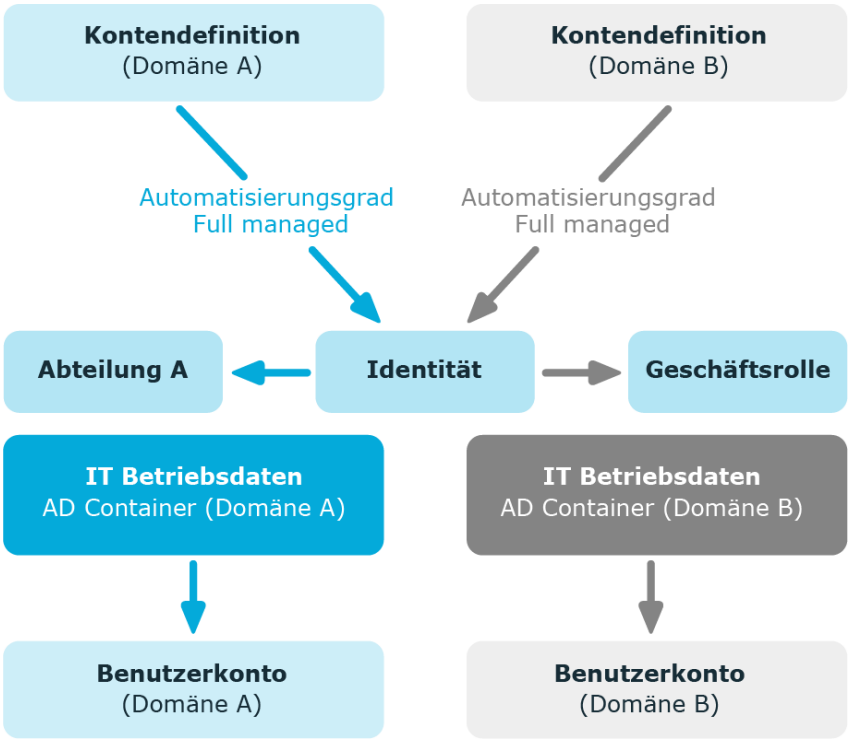


Beispiel: Identitäten können in mehreren Domänen ein Benutzerkonto besitzen

In einer Active Directory-Umgebung existieren zwei Domänen. Die Identitäten können in beiden Domänen ein Benutzerkonto besitzen. Das Benutzerkonto in Domäne A erhält die IT Betriebsdaten über die Abteilung einer Identität. Das Benutzerkonto in Domäne B erhält die IT Betriebsdaten über die primäre Geschäftsrolle einer Identität.

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 Identitäten zu Benutzerkonten

Durch die automatische Identitätenzuordnung können

- vorhandene Identitäten an Benutzerkonten zugeordnet werden
- Identitäten 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 Identitäten erfolgen. Gegebenenfalls können neue Identitäten 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 Identitätendatensätze zu erstellen.

Schalten Sie das Verfahren im laufenden Betrieb ein, dann erfolgt ab diesem Zeitpunkt die automatische Zuordnung der Identitäten 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 Identitäten zu Benutzerkonten bleiben bestehen.

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

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

- Aktivieren Sie im Designer die Konfigurationsparameter für die automatische Zuordnung der Identitäten zu Benutzerkonten und wählen Sie den gewünschten Modus aus.
- Definieren Sie die Suchkriterien für die Identitätenzuordnung.
- Sollen durch die automatische Identitätenzuordnung 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 Identität verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen Synchronisation der Fall.

Verwandte Themen

- Behandlung von Identitäten und Benutzerkonten auf Seite 7
- Konfigurieren der automatischen Identitätenzuordnung auf Seite 24

- Bearbeiten der Suchkriterien für die automatische Identitätenzuordnung auf Seite 26
- Anpassen der Skripte für die automatische Identitätenzuordnung auf Seite 31

Konfigurieren der automatischen Identitätenzuordnung

In der One Identity Manager Standardinstallation wird die automatische Zuordnung von Identitäten 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 Identitätenzuordnung wirkt, wenn Benutzerkonten neu angelegt oder aktualisiert werden.

Außerhalb der Synchronisation gilt:

- Die automatische Identitätenzuordnung 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 Identitätenzuordnung:

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

Jeder Konfigurationsparameter kennt die zulässigen Modi:

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

  HINWEIS: Dieser Modus steht nicht für alle Zielsystemtypen zur Verfügung.
- **SEARCH AND CREATE**: Ist dem Benutzerkonto keine Identität zugeordnet, wird anhand definierter Kriterien nach einer passenden Identität gesucht und die gefundene Identität dem Benutzerkonto zugeordnet. Wird keine Identität gefunden, so werden eine neue Identität angelegt, einige Eigenschaften initialisiert und die

Identität dem Benutzerkonto zugeordnet.

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

Wird durch den eingesetzten Modus ein Benutzerkonto mit einer Identität 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 Identitäten erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für das Zielsystem bekannt, werden die Benutzerkonten mit den Identitäten 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 Identitätenzuordnung 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 Identitätenzuordnung

Die Kriterien für die Identitätenzuordnung werden an den Zielsystemen definiert. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Identität übereinstimmen müssen, damit die Identität 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 Identitätenzuordnung** (`AccountToPersonMatchingRule`) der Zielsystem-Tabelle geschrieben.

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

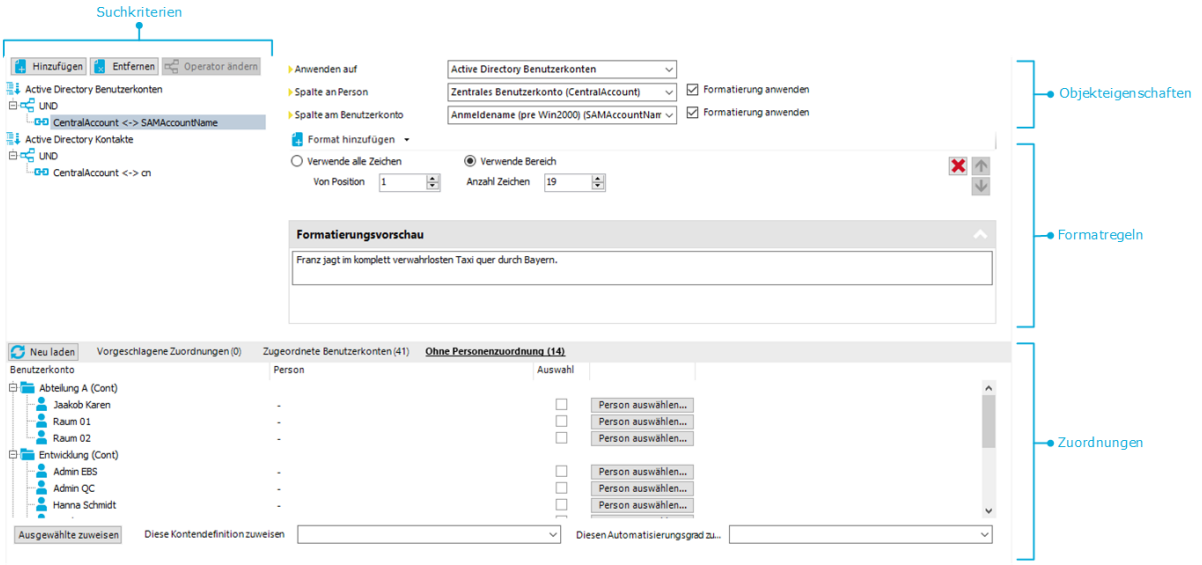
HINWEIS: Die Objektdefinitionen für Benutzerkonten, auf welche die Suchkriterien angewendet werden können, sind vordefiniert. Sollten Sie weitere Objektdefinitionen benötigen, um beispielsweise die Vorauswahl der Benutzerkonten weiter einzuschränken, erzeugen Sie im Designer die entsprechenden kundenspezifische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

Detaillierte Informationen zum Thema

- Suchkriterien für die Identitätenzuordnung definieren auf Seite 27
- Identitäten suchen und direkt an Benutzerkonten zuordnen auf Seite 30

Suchkriterien für die Identitätenzuordnung definieren

Abbildung 5: Suchkriterien für die Identitätenzuordnung



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

Um ein neues Suchkriterium für die Identitätenzuordnung 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 Identitätenzuordnung 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 Objekt-definitionen benötigen, um beispielsweise die Vorauswahl der Benutzerkonten weiter einzuschränken, erzeugen Sie im Designer die entsprechenden kunden-spezifische 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 Identität**: 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 Identität 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 3: Formatvorlagen

Formatvorlage	Bedeutung
Zeichenbereich	Zeichen der Zeichenkette, die als Suchkriterium genutzt werden sollen.
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 Identitäten an Notes Benutzerkonten zuzuordnen, müssen sowohl der Nachname als auch der Vorname von Identität und Benutzerkonto identisch sein. Folgende Tabellenspalten werden gemappt:

UND

Person.Firstname - NotesUser.Firstname

Person.LastName - NotesUser.LastName

Beispiel: ODER-Verknüpfung

Um Identitäten an Active Directory Benutzerkonten zuzuordnen, müssen entweder das zentrale Benutzerkonto der Identität und der Anmeldename des Benutzerkontos identisch sein oder der vollständige Name der Identität 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.

Verwandte Themen

- Identitäten suchen und direkt an Benutzerkonten zuordnen auf Seite 30

Identitäten suchen und direkt an Benutzerkonten zuordnen

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

- **Vorgeschlagene Zuordnungen**: Die Ansicht listet alle Benutzerkonten auf, denen der One Identity Manager eine Identität zuordnen kann. Dazu werden die Identitäten angezeigt, die durch die Suchkriterien ermittelt und zugeordnet werden können.
- **Zugeordnete Benutzerkonten**: Die Ansicht listet alle Benutzerkonten auf, denen eine Identität zugeordnet ist.
- **Ohne Identitätenzuordnung**: Die Ansicht listet alle Benutzerkonten auf, denen keine Identität zugeordnet ist und für die über die Suchkriterien keine passende Identität ermittelt werden kann.

HINWEIS: Um deaktivierte Benutzerkonten oder deaktivierte Identitäten in den Ansichten anzuzeigen, aktivieren Sie die Option **Auch gesperrte Benutzerkonten werden verbunden**.

Wenn Sie eine deaktivierte Identität an ein Benutzerkonto zuordnen, wird das Benutzerkonto, abhängig von der Konfiguration, unter Umständen gesperrt oder gelöscht.

Um Suchkriterien auf die Benutzerkonten anzuwenden

- Im unteren Bereich des Formulars **Suchkriterien für die Identitätenzuordnung 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 Identität geöffnet und Sie können die Stammdaten einsehen.

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

Um Identitäten direkt an Benutzerkonten zuzuordnen

- Klicken Sie **Vorgeschlagene Zuordnungen**.
  1. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die vorgeschlagene Identität 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 Identitäten zugeordnet. Wenn eine Kontendefinition ausgewählt wurde, wird diese an alle ausgewählten Benutzerkonten zugeordnet.

- ODER -

- Klicken Sie **Ohne Identitätenzuordnung**.
  1. Klicken Sie **Identität auswählen** für das Benutzerkonto, dem eine Identität zugeordnet werden soll. Wählen Sie eine Identität aus der Auswahlliste.
  2. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die ausgewählten Identitäten 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 Identitäten zugeordnet, die in der Spalte **Identität** 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 Zuordnungen zu Identitäten 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 Identitäten entfernt.

Anpassen der Skripte für die automatische Identitätenzuordnung

Die automatische Identitätenzuordnung wird durch Skripte gesteuert. Diese Skripte ordnen im Modus **SEARCH** anhand der definierten Suchkriterien vorhandene Identitäten an die Benutzerkonten zu. Darüber hinaus definieren die Skripte für den Modus **CREATE** die Eigenschaften, die bei Erzeugung einer neuen Identität 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 Identitätenzuordnung oder die Eigenschaften der neu zu erzeugenden Identitäten 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 Identitätenzuordnung im Modus **CREATE** werden einige Eigenschaften des Benutzerkontos an die neue Identität übergeben. Diese Identitäteneigenschaften werden ebenfalls über die Skripte definiert. Die Initialisierung von Eigenschaften bei der Erzeugung einer Identität 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 Identität erläutert.

Beispiel:

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

Bildungsregel auf `ADSAccount.Surname`:

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

Erfolgt eine Änderung des Nachnamens der Identität 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 Identität zur Hilfe genommen werden, indem diese Beziehungen rückwärts aufgelöst werden. Der Nachname der Identität kann durch den Nachnamen des Active Directory Benutzerkontos bestückt werden. Damit können also bereits einige Vorbesetzungen für die Identität automatisch generiert werden. Allerdings können nur eineindeutige Beziehungen aufgelöst werden.

Beispiel:

Der Anzeigename eines Active Directory Benutzerkontos soll aus dem Nachnamen und dem Vornamen einer Identität 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 Identitäteneigenschaften 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 Identitäten und Benutzerkonten

Der Umgang mit Identitäten, vor allem beim dauerhaften oder zeitweisen Ausscheiden einer Identität aus dem Unternehmen, wird in den einzelnen Unternehmen unterschiedlich gehandhabt. Es gibt Unternehmen, die Identitäten nie löschen, sondern nur deaktivieren, wenn sie das Unternehmen verlassen. Andere Unternehmen wollen Identitäten 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 Identitäten deaktiviert oder gelöscht werden, ist abhängig von der Art der Verwaltung der Benutzerkonten.

Es gelten folgende Szenarien:

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

Detaillierte Informationen zum Thema

- Zeitweilige Deaktivierung von Identitäten auf Seite 34
- Dauerhafte Deaktivierung von Identitäten auf Seite 35
- Verzögertes Löschen von Identitäten auf Seite 37
- Deaktivieren und Löschen über Kontendefinitionen auf Seite 38
- Behandlung von Gruppenmitgliedschaften auf Seite 42

Zeitweilige Deaktivierung von Identitäten

Die Identität 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 Identität 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 Identitäten 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 Identität und ihre Benutzerkonten wieder. Benutzerkonten einer Identität, die bereits vor einer zeitweiligen Deaktivierung der Identität deaktiviert waren, werden nach Ablauf des Zeitraumes ebenfalls wieder aktiviert.

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

- Legen Sie an den Kontendefinitionen fest, welche Auswirkungen die zeitweilige Deaktivierung von Identitäten 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 Identitäten 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 Identitäten die Gruppenmitgliedschaften der Benutzerkonten erhalten bleiben oder entfernt werden.

Szenario: Benutzerkonten sind mit Identitäten 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 Identität gesperrt. Ist der Konfigurationsparameter deaktiviert, haben die Eigenschaften der verbundenen Identität 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 Identitäten auf Seite 35
- Verzögertes Löschen von Identitäten auf Seite 37
- Deaktivieren und Löschen über Kontendefinitionen auf Seite 38
- Behandlung von Gruppenmitgliedschaften auf Seite 42

Dauerhafte Deaktivierung von Identitäten

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

Die Auswirkungen der dauerhaften Deaktivierung einer Identität sind:

- Die Identität kann nicht als Manager an Identitäten zugewiesen werden.
- Die Identität kann nicht als Verantwortlicher an Rollen zugewiesen werden.

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

Die dauerhafte Deaktivierung einer Identität wird ausgelöst über:

- die Aufgabe **Identität 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 Identitäten sperren**. Dieser Zeitplan prüft das Austrittsdatum und setzt bei Erreichen des Austrittsdatums die Option **Dauerhaft deaktiviert**.
  - Die Aufgabe **Identität erneut aktivieren** sorgt dafür, dass die Identität wieder aktiviert wird.
- den Zertifizierungsstatus **Abgelehnt**

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

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

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

- Legen Sie an den Kontendefinitionen fest, welche Auswirkungen die dauerhafte Deaktivierung von Identitäten 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 Identitäten 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 Identität die Gruppenmitgliedschaften der Benutzerkonten erhalten bleiben oder entfernt werden.

Szenario: Benutzerkonten sind mit Identitäten 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 Identität gesperrt. Ist der Konfigurationsparameter deaktiviert, haben die Eigenschaften der verbundenen Identität 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 Identitäten auf Seite 34
- Verzögertes Löschen von Identitäten auf Seite 37
- Deaktivieren und Löschen über Kontendefinitionen auf Seite 38
- Behandlung von Gruppenmitgliedschaften auf Seite 42

Verzögertes Löschen von Identitäten

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

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

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

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

- Legen Sie an den Kontendefinitionen fest, welche Auswirkungen das Löschen von Identitäten 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 Identitäten 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 Identität die Gruppenmitgliedschaften der Benutzerkonten erhalten bleiben oder entfernt werden.

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

- Implementieren Sie unternehmensspezifische Prozesse, um die verbundenen Benutzerkonten zu löschen. Eine Identität 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 Identitäten auf Seite 34
- Dauerhafte Deaktivierung von Identitäten auf Seite 35
- Deaktivieren und Löschen über Kontendefinitionen auf Seite 38
- Behandlung von Gruppenmitgliedschaften auf Seite 42

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 Identitäten 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 11.

Zuweisung von Kontendefinitionen an Identitäten

Für jede Kontendefinition wird festgelegt, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Identität auf Zuweisung der Kontendefinition selbst auswirken soll. Die Einstellungen eventueller Vorgängerkontendefinitionen werden dabei überschrieben.

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

> WICHTIG: Solange eine Kontendefinition für eine Identität wirksam ist, behält die Identität 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 4: Stammdaten einer Kontendefinition zum Zuweisungsverhalten der Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition bei dauerhafter Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Identitäten. 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 Identitäten. 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 Identitäten. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.

Eigenschaft	Beschreibung
	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 Identitäten. 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.

Behandlung von Benutzerkonten von Identitäten

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

Um bei Deaktivierung oder Löschen einer Identität die Berechtigungen zu entziehen, können die Benutzerkonten der Identität gesperrt werden. Wird die Identität 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 5: Stammdaten eines Automatisierungsgrades zur Behandlung von Benutzerkonten

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

Vererbung von Gruppenmitgliedschaften an die Benutzerkonten der Identitäten

Für jeden Automatisierungsgrad wird festgelegt, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Identität auf

die Gruppenmitgliedschaften der Benutzerkonten auswirken soll.

Ist eine Identität 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 Identität gesperrt sind und somit auch nicht in Verteilerlisten Mitglied sein dürfen. Während der Zeit der Deaktivierung sollten keine Vererbungsvorgänge für diese Identitäten berechnet werden. Bestehende Gruppenmitgliedschaften werden gelöscht.

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

Tabelle 6: Stammdaten einer Automatisierungsgrades zur Behandlung von Gruppenmitgliedschaften

Eigenschaft	Beschreibung
Gruppen bei zeitweiliger Deaktivierung beibehalten	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Identitäten ihre Gruppenmitgliedschaften behalten sollen.
Gruppen bei dauerhafter Deaktivierung beibehalten	Gibt an, ob Benutzerkonten dauerhaft deaktivierter Identitäten Gruppenmitgliedschaften erben sollen.
Gruppen bei verzögertem Löschen beibehalten	Gibt an, ob die Benutzerkonten zum Löschen markierter Identitäten ihre Gruppenmitgliedschaften behalten sollen.
Gruppen bei Sicherheitsgefährdung beibehalten	Gibt an, ob die Benutzerkonten von sicherheitsgefährdenden Identitäten 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 42.

Verwandte Themen

- Zeitweilige Deaktivierung von Identitäten auf Seite 34
- Dauerhafte Deaktivierung von Identitäten auf Seite 35
- Verzögertes Löschen von Identitäten 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 Identitäten 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 Identitäten behandelt werden sollen.

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

- Wird eine Identität 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 Identitäten behandelt werden sollen.

  Die Einstellung ist wirksam für Benutzerkonten, die mit Identitäten 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 Identitäten 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 Identität 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 Identitäten 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. Wahlen 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 Identitäten auf Seite 34
- Dauerhafte Deaktivierung von Identitäten auf Seite 35

- Deaktivieren und Löschen über Kontendefinitionen auf Seite 38
- Verzögertes Löschen von Identitäten auf Seite 37

2

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 45
- Besonderheiten bei der Abbildung von Objekteigenschaften auf Seite 52
- One Identity Manager Benutzer für die Verwaltung von Zielsystemen im Unified Namespace auf Seite 52
- Unified Namespace Objekte anzeigen auf Seite 53
- Berichte über ein Zielsystem im Unified Namespace auf Seite 54
- Berichte über alle Zielsysteme im Unified Namespace auf Seite 57

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 Compliancеprüfungen 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
OneLogin	OLGAPIDomain

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
OneLogin	OLGUser

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

Zielsystemtyp	Tabelle
LDAP	LDAPGroup
Kundendefinierte Zielsysteme	UNSGroupB, UNSGroupB1, UNSGroupB2, UNSGroupB3
Unix	UNXGroup
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
OneLogin	OLGApplication, OLGRole

Berechtigungselemente (`UNSItem`)

Die Sicht `UNSItem` bildet zusätzliche Berechtigungselemente der Zielsysteme ab.

Zielsystemtyp	Tabelle
Kundendefinierte Zielsysteme	UNSItemB
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,

Zielsystemtyp	Tabelle
	UNSAccounBInUNSGroupB1, UNSAccounBInUNSGroupB2, UNSAccounBInUNSGroupB3, UNSAccounBHasUNSGroupB, UNSAccounBHasUNSGroupB1, UNSAccounBHasUNSGroupB2, UNSAccounBHasUNSGroupB3
Unix	UNXAccountInUNXGroup
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
OneLogin	OLGUserHasOLGApplication, OLGUserInOLGRole

Zuweisungen Berechtigungselemente (`UNSAccountHasUNSItem`)

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

Zielsystemtyp	Tabelle
Kundendefinierte Zielsysteme	UNSAccountBHasUNSItemB
Cloud Zielsysteme	CSMUserHasItem

Zuweisungen Systemberechtigungen (`UNSGroupInUNSGroup`)

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

Zielsystemtyp	Tabelle
Active Directory	ADSGroupInADSGroup

Zielsystemtyp	Tabelle
SharePoint	SPSGroupHasSPSRLAsgn
HCL Domino	NotesGroupInGroup
SAP R/3	SAPProfileInSAPProfile, SAPRoleInSAPRole, SAPProfileInSAPRole
LDAP	LDAPGroupInLDAPGroup
Kundendefinierte Zielsysteme	UNSGroupBInUNSGroupB, UNSGroupBInUNSGroupB1, UNSGroupBInUNSGroupB2, UNSGroupBInUNSGroupB3
Azure Active Directory	AADGroupInGroup
Exchange Online	O3EDLInDL
Google Workspace	GAPGroupInGroup
Cloud Zielsysteme	CSMGroupInGroup, CSMGroupInGroup1, CSMGroupInGroup2, CSMGroupInGroup3

Zuweisungen Berechtigungselemente (`UNSGroupHasUNSItem`)

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

Zielsystemtyp	Tabelle
Kundendefinierte Zielsysteme	UNSGroupBHasUNSItemB
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

Zielsystemtyp	Tabelle
Unix	UNXGroupExclusion
Azure Active Directory	AADGroupExclusion, AADSubSkuExclusion
Google Workspace	GAPGroupExclusion
Cloud Zielsysteme	CSMGroupExclusion, CSMGroup1Exclusion, CSMGroup2Exclusion, CSMGroup3Exclusion
Oracle E-Business Suite	EBSRespExclusion
Privileged Account Management	PAGUsrGroupExclusion
OneLogin	OLGApplicationExclusion, OLGRoleExclusion

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 7: Benutzer

Benutzer	Aufgaben
Zielsystemadministratoren	Die Zielsystemadministratoren müssen der Anwendungsrolle **Zielsysteme | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen. • Legen die Zielsystemverantwortlichen fest. • Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein. • Legen fest, welche Anwendungsrollen für Zielsystemverantwortliche sich ausschließen. • Berechtigen weitere Identitäten als Zielsystemadministratoren. • Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Unified Namespace** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Erhalten eine zielsystemübergreifende Sicht auf die Objekte der angeschlossenen Zielsysteme. • Können zielsystemübergreifende Berichte erstellen. Sind die Benutzer gleichzeitig Zielsystemverantwortliche der zugrunde liegenden Zielsysteme, können sie diese Zielsysteme über den Unified Namespace verwalten.
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. 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 angebundenen 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 8: 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.

Bericht	Bereitgestellt für	Beschreibung
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 Identitäten befinden, die im ausgewählten Container mindestens ein Benutzerkonto besitzen.
Übersicht aller Zuweisungen	Systemberechtigung	Der Bericht ermittelt alle Rollen, in denen sich Identitäten 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 Identitäten, die einem Benutzerkonto dieser Systemberechtigung zugeordnet sind, einschließlich der Dauer der Mitgliedschaft.

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.
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. 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 überdurchschnittliche Anzahl an Systemberechtigungen anzeigen	Zielsystem	Der Bericht enthält alle Benutzerkonten, die eine überdurchschnittliche Anzahl an Systemberechtigungen besitzen.
Identitäten mit mehreren Benutzerkonten anzeigen	Zielsystem	Der Bericht zeigt alle Identitäten, 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.

Bericht	Bereitgestellt für	Beschreibung
Übersicht aller Zuweisungen	Zielsystem	Der Bericht ermittelt alle Rollen, in denen sich Identitäten 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 Identität 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 9: Berichte zur Datenqualität aller Zielsysteme

Bericht	Beschreibung
Unverbundene Benutzerkonten aus allen Zielsystemen	Der Bericht zeigt alle Benutzerkonten, denen keine Identität 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 überdurchschnittliche Anzahl an System-	Der Bericht enthält alle Benutzerkonten, die eine überdurchschnittliche Anzahl an Systemberechtigungen besitzen. Den Bericht finden Sie in der Kategorie **Mein**

Bericht	Beschreibung
berechtigungen	**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**.

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

Technische Unterstützung steht für 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

Index

Z