



One Identity Manager 9.2

Administrationshandbuch für
Behavior Driven Governance

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 Behavior Driven Governance
Aktualisiert - 02. Oktober 2023, 10:31 Uhr

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

Inhalt

Überblick zum Behavior Driven Governance	4
Behavior Driven Governance für OneLogin	6
Voraussetzungen für den automatischen Entzug ungenutzter OneLogin Anwendungen	7
Ungenutzte Zugänge zu OneLogin Anwendungen ermitteln	8
Ungenutzte OneLogin Anwendungen ermitteln	12
Zuweisungen von OneLogin Anwendungen an OneLogin Rollen ermitteln	16
Behavior Driven Governance für Privileged Account Management	19
Behavior Driven Governance für Zielsysteme im Unified Namespace	21
Ungenutzte Benutzerkonten ermitteln und deaktivieren	22
Ungenutzte Benutzerkonten ermitteln und löschen	23
Anhang: Konfigurationsparameter für Behavior Driven Governance	26
Über uns	27
Kontaktieren Sie uns	27
Technische Supportressourcen	27
Index	28

Überblick zum Behavior Driven Governance

Behavior Driven Governance gibt IT-Administratoren und Compliance-Verantwortlichen die Möglichkeit Berechtigungen auf Grundlage des Nutzungsverhaltens zu administrieren. So können Berechtigungen, die nicht mehr benötigt werden, identifiziert und entfernt werden. Regelmäßige Überprüfungen und Rezertifizierungen dieser Berechtigungen bewirken, dass dauerhaft nur noch tatsächlich benötigte Berechtigungen vergeben sind.

One Identity Manager stellt verschiedene Standard-Richtlinien und Prozesse für Behavior Driven Governance bereit.

Integration mit OneLogin

Wenn Daten von OneLogin Cloud Directory mit One Identity Manager synchronisiert werden, kann der Zugang zu OneLogin Anwendungen abhängig vom Nutzungsverhalten rezertifiziert und administriert werden. Dafür werden Informationen aus der OneLogin Änderungshistorie genutzt. Für folgende Aufgaben stehen Standard-Richtlinien bereit:

- Ermittlung von Zugängen zu OneLogin Anwendungen, die für einen definierten Zeitraum nicht genutzt wurden
- Ermittlung von OneLogin Anwendungen, die in einem definierten Zeitraum von niemandem genutzt wurden
- Ermittlung von OneLogin Anwendungen, die mehr als einer OneLogin Rolle zugewiesen sind
- Ermittlung von OneLogin Rollen, die Zugang zu mehr als einer OneLogin Anwendung gewähren

Ungenutzte Anwendungen können bei entsprechender Konfiguration automatisch entfernt werden.

Integration mit anderen Zielsystemen des Unified Namespace

Für Zielsysteme, die im Unified Namespace abgebildet sind, können über eine Standard-Unternehmensrichtlinie alle Benutzerkonten ermittelt werden, die für einen definierten Zeitraum nicht genutzt wurden. Mit diesen Informationen können Administratoren die Zugangsberechtigungen zu den Zielsystemen überprüfen und korrigieren.

Sicherheitsrisiken, die mit ungenutzten, aber aktiven Benutzerkonten verbunden sind,

können so verringert werden. Voraussetzung ist, dass diese Zielsysteme eine Information über die Nutzungsdauer der Benutzerkonten bereitstellen und diese Daten synchronisiert werden.

Vorausgesetzte Module

Behavior Driven Governance kann genutzt werden, wenn folgende Module installiert sind:

- Modul Unternehmensrichtlinien
- Modul Attestierung
- Zielsystem Basismodul
- OneLogin Modul

Detaillierte Informationen zum Thema

- [Behavior Driven Governance für OneLogin auf Seite 6](#)
- [Behavior Driven Governance für Zielsysteme im Unified Namespace auf Seite 21](#)

Behavior Driven Governance für OneLogin

HINWEIS: Die Funktionalität steht zur Verfügung, wenn das OneLogin Modul installiert ist.

One Identity Manager stellt verschiedene Unternehmensrichtlinien und Attestierungsrichtlinien bereit, um den Zugang zu OneLogin Anwendungen abhängig vom Nutzungsverhalten zu überprüfen und zu rezertifizieren oder zu entfernen. Folgende Szenarien können damit behandelt werden:

- Zugänge zu OneLogin Anwendungen, die nicht genutzt werden
OneLogin Benutzer sollten die ihnen zugewiesenen Anwendungen mindestens einmal innerhalb eines definierten Zeitraums nutzen. Wenn eine Anwendung laut Änderungshistorie in diesem Zeitraum nicht genutzt wurde, soll die Zuweisung der Anwendung an das OneLogin Benutzerkonto rezertifiziert oder gelöscht werden.
Über eine Unternehmensrichtlinie werden alle ungenutzten Zugänge zu OneLogin Anwendungen ermittelt. Ausnahmegenehmiger werden über die betroffenen Anwendungen und Benutzerkonten informiert. Parallel dazu wird ein Rezertifizierungsverfahren gestartet. Im Lauf der Rezertifizierung erklären die Benutzer und deren Manager oder die Zielsystemverantwortlichen, ob die Anwendungen weiterhin benötigt werden. Falls nicht, kann der Zugang zu ungenutzten Anwendungen anschließend automatisch oder manuell entfernt werden.
- OneLogin Anwendungen, die von niemandem genutzt werden
Anwendungen sollten mindestens einmal innerhalb eines definierten Zeitraums von mindestens einem OneLogin Benutzer genutzt werden. Wenn eine Anwendung laut Änderungshistorie in diesem Zeitraum nicht genutzt wurde, können die Zuweisungen der Anwendung an OneLogin Benutzerkonten rezertifiziert oder gelöscht werden.
Über eine Unternehmensrichtlinie werden alle ungenutzten OneLogin Anwendungen ermittelt. Ausnahmegenehmiger werden über die betroffenen Anwendungen informiert. Über eine Rezertifizierung kann geklärt werden, ob die Anwendungen noch benötigt werden. Der Zugang zu ungenutzten Anwendungen kann anschließend automatisch oder manuell entfernt werden.
- Nicht eindeutige Zuordnung von OneLogin Anwendungen an OneLogin Rollen
Der Zugang von OneLogin Benutzern zu Anwendungen wird über Rollen geregelt. Wenn der Zugang entfernt werden soll, muss die Zuweisung der OneLogin Rollen an

die Benutzerkonten entfernt werden. Um dabei keine anderen, gegebenenfalls noch benötigten Berechtigungen zu entfernen, darf den Rollen nur genau eine Anwendung zugewiesen sein. Wenn die Zuordnung von Anwendungen zu Rollen eindeutig ist, können ungenutzte Zugänge zu Anwendungen automatisch entfernt werden.

Über Unternehmensrichtlinien werden alle OneLogin Rollen ermittelt, denen mehr als eine Anwendung zugewiesen ist, sowie alle Anwendungen, die mehr als einer Rolle zugewiesen sind. Ausnahmegenehmiger werden über die betroffenen Rollen und Anwendungen informiert und können geeignete Maßnahmen veranlassen.

Nach welchem Zeitraum Anwendungen als ungenutzt betrachtet werden, ist im Konfigurationsparameter **TargetSystem | OneLogin | UnusedApplicationThresholdInDays** festgelegt. Der Standardwert ist 90 Tage.

Ausführliche Informationen zur Abbildung von OneLogin Anwendungen, OneLogin Benutzerkonten und OneLogin Rollen finden Sie im *One Identity Manager Administrationshandbuch für die Integration mit OneLogin Cloud Directory*.

Detaillierte Informationen zum Thema

- [Ungenutzte Zugänge zu OneLogin Anwendungen ermitteln](#) auf Seite 8
- [Ungenutzte OneLogin Anwendungen ermitteln](#) auf Seite 12
- [Zuweisungen von OneLogin Anwendungen an OneLogin Rollen ermitteln](#) auf Seite 16
- [Voraussetzungen für den automatischen Entzug ungenutzter OneLogin Anwendungen](#) auf Seite 7

Verwandte Themen

- [Behavior Driven Governance für Zielsysteme im Unified Namespace](#) auf Seite 21

Voraussetzungen für den automatischen Entzug ungenutzter OneLogin Anwendungen

Um den Zugriff von OneLogin Benutzerkonten auf OneLogin Anwendungen automatisch zu entfernen, ermittelt One Identity Manager die OneLogin Rollen, über welche die Anwendungen zugewiesen wurden. Wenn einer so ermittelten Rolle genau nur die ungenutzte Anwendung zugewiesen ist, kann die Mitgliedschaft des Benutzerkontos in der Rolle entfernt werden. Damit verliert das Benutzerkonto den Zugang zu der Anwendung. Wenn einer OneLogin Rolle mehrere Anwendungen zugewiesen sind, wird die Mitgliedschaft nicht automatisch gelöscht, um sicherzustellen, dass der Zugang zu allen anderen Anwendungen in dieser Rolle erhalten bleibt.

HINWEIS: Direkte Zuweisungen von Anwendungen an Benutzerkonten können im One Identity Manager nicht entfernt werden. Direkte Zuweisungen müssen nach

| negativer Attestierung im Zielsystem manuell entfernt werden.

Voraussetzungen

Um ungenutzte Anwendungen zu ermitteln und zu rezertifizieren, müssen folgende Voraussetzungen gegeben sein:

- Die OneLogin Änderungshistorie wird synchronisiert. Es werden mindestens Ereignisse mit den Typen 5, 6, 7, 8, 11, 22, 29 synchronisiert (event_type_id=5,6,7,8,11,22,29).
- Der Konfigurationsparameter **TargetSystem | OneLogin | UnusedApplicationThresholdInDays** ist aktiviert. Der Wert gibt an, nach wieviel Tagen ohne Zugriff eine OneLogin Anwendung als ungenutzt betrachtet wird.
- Den Identitäten, die mit den Benutzerkonten verbunden sind, muss ein Manager zugeordnet sein.
- Es müssen Zielsystemverantwortliche für OneLogin festgelegt sein.

Um den Zugang zu ungenutzten Anwendungen automatisch zu entfernen, müssen folgende Voraussetzungen geschaffen werden:

- OneLogin Anwendungen sind ausschließlich über OneLogin Rollen an die Benutzerkonten zugewiesen. Nur diese Zuweisungen können im One Identity Manager automatisch oder manuell entfernt werden.
- An OneLogin Rollen ist jeweils nur eine OneLogin Anwendung zugewiesen.

TIPP: Nutzen Sie die Unternehmensrichtlinie **Allen OneLogin Rollen ist nur eine OneLogin Anwendung zugewiesen**, um Rollen mit mehreren Anwendungen zu identifizieren.

Detaillierte Informationen zum Thema

- [Ungenutzte Zugänge zu OneLogin Anwendungen ermitteln](#) auf Seite 8
- [Ungenutzte OneLogin Anwendungen ermitteln](#) auf Seite 12
- [Zuweisungen von OneLogin Anwendungen an OneLogin Rollen ermitteln](#) auf Seite 16

Ungenutzte Zugänge zu OneLogin Anwendungen ermitteln

OneLogin Benutzer sollten die ihnen zugewiesenen Anwendungen mindestens einmal innerhalb eines definierten Zeitraums nutzen. Über eine Standard-Unternehmensrichtlinie werden alle Zuweisungen von OneLogin Anwendungen an Benutzerkonten, die laut Änderungshistorie in diesem Zeitraum nicht genutzt wurden, ermittelt. Ausnahmegenehmiger werden über die betroffenen Anwendungen und Benutzerkonten informiert. Parallel dazu wird ein Rezertifizierungsverfahren gestartet. Im Lauf der Rezertifizierung erklären die Benutzer und deren Manager oder die

Zielsystemverantwortlichen, ob die Anwendungen weiterhin benötigt werden. Falls nicht, kann der Zugang zu ungenutzten Anwendungen anschließend automatisch oder manuell entfernt werden.

Zuweisungen werden als ungenutzt identifiziert, wenn folgende Bedingungen zutreffen:

- Die Zuweisung ist wirksam (OLGUserHasApplication.XIsInEffect=1).
- Der OneLogin Benutzer hat sich mindestens einmal an OneLogin angemeldet (OLGUser.LastLogin).
- Die Zeitspanne zwischen dem letzten Anmeldedatum an der Anwendung (OLGEvent.CreatedAt) und dem aktuellen Datum ist größer oder gleich dem Wert des Konfigurationsparameters **TargetSystem | OneLogin | UnusedApplicationThresholdInDays**.

- ODER -

In der Änderungshistorie gibt kein Anmeldedatum an der Anwendung für das Benutzerkonto. Der Benutzer hat die Anwendung folglich noch nie genutzt.

Um ungenutzte Zuweisungen zu ermitteln und zu rezertifizieren

1. (Optional) Konfigurieren Sie den automatischen Entzug von Berechtigungen.
Abhängig vom Verfahren, mit dem OneLogin Benutzerkonten an OneLogin Rollen zugewiesen werden (direkt, per IT Shop-Bestellung, über hierarchische Rollen oder Systemrollen), müssen verschiedene Konfigurationsparameter aktiviert werden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*.
2. (Optional) Prüfen Sie, ob Benachrichtigungen über Richtlinienverletzungen und Benachrichtigungen im Attestierungsvorgang eingerichtet sind.
Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für Unternehmensrichtlinien* und im *One Identity Manager Administrationshandbuch für Attestierungen*.
3. (Optional) Weisen Sie der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Ausnahmegenehmiger** die Identitäten zu, die über ungenutzte OneLogin Anwendungen informiert werden sollen und gegebenenfalls Ausnahmen genehmigen dürfen.
 1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Ausnahmegenehmiger**.
 2. Wählen Sie die Aufgabe **Identitäten zuweisen**.
 3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Identitäten zu.
TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Identitäten entfernen.
Um eine Zuweisung zu entfernen
 - Wählen Sie die Identität und doppelklicken Sie .
4. Speichern Sie die Änderungen.

4. (Optional) Um für die Rezertifizierung den Zeitraum zu ändern, nachdem eine Anwendung als ungenutzt behandelt wird, bearbeiten Sie die Attestierungsrichtlinie **Attestierung von ungenutzten Zugängen zu OneLogin Anwendungen** im Web Portal.

- Bearbeiten Sie die Bedingung **Ungenutzt für x Tage** und ändern Sie die Anzahl der Tage.

Ausführliche Informationen dazu finden Sie im *One Identity Manager Web Portal Anwenderhandbuch*.

5. Aktivieren Sie die Arbeitskopie der Unternehmensrichtlinie **Zugänge zu OneLogin Anwendungen werden regelmäßig genutzt**.

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien > Vordefiniert**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Arbeitskopie aktivieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Aktivieren Sie die originale Richtlinie. Bestätigen Sie die Abfrage mit **Ja**.

Die Richtlinienprüfung wird anschließend gestartet.

TIPP: Wenn bereits eine aktive Unternehmensrichtlinie vorhanden ist, können Sie die Richtlinienprüfung über die Aufgabe **Richtlinie neu berechnen** starten.

Durch den hinterlegten Zeitplan wird die Richtlinienprüfung einmal monatlich gestartet.

HINWEIS: Wenn Sie verhindern wollen, dass neue Richtlinienverletzungen sofort attestiert werden sollen, deaktivieren Sie **Attestierung für neue Richtlinienverletzungen sofort starten**.

6. (Optional) Um genehmigte ungenutzte Zuweisungen regelmäßig zu rezertifizieren, weisen Sie der Attestierungsrichtlinie **Attestierung von ungenutzten Zugängen zu OneLogin Anwendungen** einen aktivierten Zeitplan zu.

1. Wählen Sie im Manager die Kategorie **Attestierung > Attestierungsrichtlinien > Vordefiniert**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie aus der Auswahlliste **Zeitplan der Berechnung** einen aktivierten Zeitplan.
- ODER -
Klicken Sie , um einen neuen Zeitplan zu erstellen.
5. Speichern Sie die Änderungen.

Ablauf

1. Die Überprüfung der Unternehmensrichtlinie **Zugänge zu OneLogin Anwendungen werden regelmäßig genutzt** wird zeitgesteuert oder über die Aufgabe **Richtlinie neu berechnen** im Manager gestartet.
 - Es werden alle Zuweisungen von OneLogin Anwendungen an Benutzerkonten ermittelt, bei denen sich das Benutzerkonto entweder noch nie oder nicht innerhalb der festgelegten Zeitspanne angemeldet hat.
 - Ausnahmegenehmiger werden per E-Mail über die Richtlinienverletzungen benachrichtigt.
2. Für jede Zuweisung, welche die Richtlinie verletzt, wird automatisch eine Attestierung mit der Attestierungsrichtlinie **Attestierung von ungenutzten Zugängen zu OneLogin Anwendungen** gestartet.

Entscheidungsverlauf:

- a. Es wird geprüft, ob das Benutzerkonto mit einer Identität verbunden ist
 - Wenn nicht, wird die Zuweisung den Zielsystemverantwortlichen zur Attestierung vorgelegt.
- b. Die verbundene Identität bestätigt, ob die zugewiesene Anwendung benötigt wird.
- c. Der Manager der verbundenen Identität entscheidet, ob die Zuweisung erhalten bleiben soll.
- d. Wenn in einer Entscheidungsebene die Attestierung abgelehnt wurde, wird geprüft, ob die Zuweisung automatisch entfernt werden kann. Es werden alle OneLogin Rollen ermittelt, über welche die Anwendungen an das Benutzerkonto zugewiesen sind.
 - Wenn einer Rolle keine anderen Anwendungen zugewiesen sind, wird der automatische Entzug dieser Rolle initiiert. Dabei wird die Zuweisung der Rolle an das Benutzerkonto entfernt und die Änderung wird in das Zielsystem provisioniert. Damit wird dem OneLogin Benutzer die Berechtigung zur Nutzung der Anwendung entzogen.
Mit der folgenden Synchronisation wird die Zuweisung der Anwendung an das Benutzerkonto, je nach Konfiguration der Synchronisation, in der One Identity Manager-Datenbank als ausstehend markiert oder gelöscht. Führen Sie einen Zielsystemabgleich durch, um ausstehende Zuweisungen endgültig zu löschen.
- e. Wenn die Anwendung direkt an das Benutzerkonto zugewiesen ist oder über eine OneLogin Rolle Zugang zu mehreren Anwendungen gewährt wird, wird der Attestierungsvorgang den Zielsystemverantwortlichen zur finalen Bearbeitung vorgelegt.
 - Wenn die Zielsystemverantwortlichen die Attestierung ablehnen, müssen sie dafür sorgen, dass die Zuweisungen manuell entfernt werden.

Wenn der Manager oder die Zielsystemverantwortlichen die Attestierung genehmigt haben, bleibt die Zuweisung erhalten. Wenn die Zuweisung bei der folgenden zyklischen oder

manuellen Prüfung erneut als ungenutzt erkannt wird, wird sie den Attestierern erneut zur Prüfung vorgelegt.

Verwandte Themen

- [Behavior Driven Governance für OneLogin](#) auf Seite 6
- [Voraussetzungen für den automatischen Entzug ungenutzter OneLogin Anwendungen](#) auf Seite 7
- [Ungenutzte OneLogin Anwendungen ermitteln](#) auf Seite 12
- [Zuweisungen von OneLogin Anwendungen an OneLogin Rollen ermitteln](#) auf Seite 16

Ungenutzte OneLogin Anwendungen ermitteln

Anwendungen sollten mindestens einmal innerhalb eines definierten Zeitraums von mindestens einem OneLogin Benutzer genutzt werden. Über eine Standard-Unternehmensrichtlinie werden alle OneLogin Anwendungen ermittelt, die laut Änderungshistorie in diesem Zeitraum nicht genutzt wurden. Ausnahmegenehmiger werden über die betroffenen Anwendungen informiert. Über eine Rezertifizierung kann geklärt werden, ob die Anwendungen noch benötigt werden. Dabei erklären die Benutzer und deren Manager oder die Zielsystemverantwortlichen, ob die Anwendungen weiterhin benötigt werden. Falls nicht, kann der Zugang zu ungenutzten Anwendungen anschließend automatisch oder manuell entfernt werden. Die Standard-Richtlinien müssen aktiviert und unternehmensspezifisch konfiguriert werden.

Anwendungen werden als ungenutzt identifiziert, wenn folgende Bedingungen zutreffen:

- Die Anwendung ist mindestens einem OneLogin Benutzerkonto zugewiesen (OLGUserHasOLGApplication).
- Die Zeitspanne zwischen dem letzten Anmeldedatum an der Anwendung (OLGEvent.CreatedAt) und dem aktuellen Datum ist größer oder gleich dem Wert des Konfigurationsparameters **TargetSystem | OneLogin | UnusedApplicationThresholdInDays**.

- ODER -

In der Änderungshistorie gibt kein Anmeldedatum an der Anwendung für ein Benutzerkonto. Folglich hat kein Benutzer die Anwendung bisher genutzt.

Um ungenutzte Anwendungen zu ermitteln und zu rezertifizieren

1. (Optional) Konfigurieren Sie den automatischen Entzug von Berechtigungen.

Abhängig vom Verfahren, mit dem OneLogin Benutzerkonten an OneLogin Rollen zugewiesen werden (direkt, per IT Shop-Bestellung, über hierarchische Rollen oder Systemrollen), müssen verschiedene Konfigurationsparameter aktiviert werden.

Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*.

2. (Optional) Prüfen Sie, ob Benachrichtigungen über Richtlinienverletzungen und Benachrichtigungen im Attestierungsvorgang eingerichtet sind.

Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für Unternehmensrichtlinien* und im *One Identity Manager Administrationshandbuch für Attestierungen*.

3. (Optional) Weisen Sie der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Ausnahmegenehmiger** die Identitäten zu, die über ungenutzte OneLogin Anwendungen informiert werden sollen und gegebenenfalls Ausnahmen genehmigen dürfen.

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Ausnahmegenehmiger**.
2. Wählen Sie die Aufgabe **Identitäten zuweisen**.
3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Identitäten zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Identität und doppelklicken Sie .

4. Speichern Sie die Änderungen.

4. Aktivieren Sie die Arbeitskopie der Unternehmensrichtlinie **Ungenutzte OneLogin Anwendungen können entfernt werden**.

Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für Unternehmensrichtlinien*.

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien > Vordefiniert**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Arbeitskopie aktivieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Aktivieren Sie die originale Richtlinie. Bestätigen Sie die Abfrage mit **Ja**.

Die Richtlinienprüfung wird anschließend gestartet.

TIPP: Wenn bereits eine aktive Unternehmensrichtlinie vorhanden ist, können Sie die Richtlinienprüfung über die Aufgabe **Richtlinie neu berechnen** starten.

Durch den hinterlegten Zeitplan wird die Richtlinienprüfung einmal monatlich gestartet.

5. Bearbeiten Sie die Attestierungsrichtlinie **Attestierung des Zugangs zu OneLogin Anwendungen** im Web Portal.

Ausführliche Informationen dazu finden Sie im *One Identity Manager Web Portal Anwenderhandbuch*.

- a. (Optional) Um ungenutzte Anwendungen regelmäßig zu rezertifizieren, weisen Sie im Auswahlfeld **Zeitplan der Berechnung** einen aktivierten Zeitplan zu.
- b. Legen Sie fest, welche Anwendungen rezertifiziert werden sollen. Fügen Sie im Bereich **Objekte, die durch diese Attestierungsrichtlinie attestiert werden** mindestens eine weitere Bedingung hinzu.

Beispiel:

1. Wählen Sie den Bedingungstyp **Bestimmte Anwendungen** und wählen Sie eine der Anwendungen aus, die durch die Unternehmensrichtlinie als ungenutzt identifiziert wurden.
2. Fügen Sie eine weitere Bedingung mit dem Bedingungstyp **Ungenutzt für x Tage** hinzu und erfassen Sie die Anzahl der Tage, nach denen die Anwendung als ungenutzt identifiziert wird.
3. Löschen Sie die Bedingung **Alle Anwendungen**.

Wenn Sie keine Bedingung hinzufügen, werden Attestierungsvorgänge für alle Zuweisungen von OneLogin Anwendungen an OneLogin Benutzerkonten erzeugt.

- c. Aktivieren Sie die Attestierungsrichtlinie.
 - Deaktivieren Sie **Deaktiviert**.
- d. Speichern Sie die Änderungen.

Ablauf

1. Die Überprüfung der Unternehmensrichtlinie **Ungenutzte OneLogin Anwendungen können entfernt werden** wird zeitgesteuert oder über die Aufgabe **Richtlinie neu berechnen** im Manager gestartet.
 - Es werden alle OneLogin Anwendungen ermittelt, an denen sich innerhalb der festgelegten Zeitspanne kein Benutzerkonto angemeldet hat oder an denen sich noch nie ein Benutzerkonto angemeldet hat.
 - Ausnahmegenehmiger werden per E-Mail über die Richtlinienverletzungen benachrichtigt.
2. Die Attestierung mit der Attestierungsrichtlinie **Attestierung des Zugangs zu OneLogin Anwendungen** wird zeitgesteuert oder manuell im Web Portal gestartet.

Es werden alle Zuweisungen von OneLogin Anwendungen an Benutzerkonten entsprechend der konfigurierten Bedingung ermittelt.

Entscheidungsverlauf:

 - a. Es wird geprüft, ob das Benutzerkonto mit einer Identität verbunden ist
 - Wenn nicht, wird die Zuweisung den Zielsystemverantwortlichen zur Attestierung vorgelegt.

- b. Die verbundene Identität bestätigt, ob die zugewiesene Anwendung benötigt wird.
- c. Der Manager der verbundenen Identität entscheidet, ob die Zuweisung erhalten bleiben soll.
- d. Wenn in einer Entscheidungsebene die Attestierung abgelehnt wurde, wird geprüft, ob die Zuweisung automatisch entfernt werden kann. Es werden alle OneLogin Rollen ermittelt, über welche die Anwendungen an das Benutzerkonto zugewiesen sind.
 - Wenn einer Rolle keine anderen Anwendungen zugewiesen sind, wird der automatische Entzug dieser Rolle initiiert. Dabei wird die Zuweisung der Rolle an das Benutzerkonto entfernt und die Änderung wird in das Zielsystem provisioniert. Damit wird dem OneLogin Benutzer die Berechtigung zur Nutzung der Anwendung entzogen.

Mit der folgenden Synchronisation wird die Zuweisung der Anwendung an das Benutzerkonto, je nach Konfiguration der Synchronisation, in der One Identity Manager-Datenbank als ausstehend markiert oder gelöscht. Führen Sie einen Zielsystemabgleich durch, um ausstehende Zuweisungen endgültig zu löschen.
- e. Wenn die Anwendung direkt an das Benutzerkonto zugewiesen ist oder über eine OneLogin Rolle Zugang zu mehreren Anwendungen gewährt wird, wird der Attestierungsvorgang den Zielsystemverantwortlichen zur finalen Bearbeitung vorgelegt.
 - Wenn die Zielsystemverantwortlichen die Attestierung ablehnen, müssen sie dafür sorgen, dass die Zuweisungen manuell entfernt werden.

Wenn der Manager oder die Zielsystemverantwortlichen die Attestierung genehmigt haben, bleibt die Zuweisung erhalten und wird bei der folgenden zyklischen Prüfung erneut zur Rezertifizierung vorgelegt.

Verwandte Themen

- [Behavior Driven Governance für OneLogin](#) auf Seite 6
- [Voraussetzungen für den automatischen Entzug ungenutzter OneLogin Anwendungen](#) auf Seite 7
- [Ungenutzte Zugänge zu OneLogin Anwendungen ermitteln](#) auf Seite 8
- [Zuweisungen von OneLogin Anwendungen an OneLogin Rollen ermitteln](#) auf Seite 16

Zuweisungen von OneLogin Anwendungen an OneLogin Rollen ermitteln

Der Zugang von OneLogin Benutzern zu Anwendungen wird über Rollen geregelt. Um den Zugang zu OneLogin Anwendungen automatisiert administrieren zu können, darf an eine OneLogin Rolle genau nur eine OneLogin Anwendung zugewiesen sein. Wenn diese Anwendung nicht mehr benötigt wird, kann die Mitgliedschaft in der Rolle entfernt werden, ohne gleichzeitig den Zugang zu anderen Anwendungen zu entziehen. Gleichermaßen sollte eine Anwendung genau nur einer OneLogin Rolle zugewiesen sein. Wenn diese Anwendung nicht mehr benötigt wird, muss damit nur die Mitgliedschaft in einer Rolle entfernt werden.

Mit Hilfe von Standard-Unternehmensrichtlinien können Sie prüfen, ob diese Voraussetzungen für den automatischen Entzug von Berechtigungen erfüllt sind. Ausnahmegenehmiger werden über die betroffenen Rollen und Anwendungen informiert und können geeignete Maßnahmen veranlassen.

Um OneLogin Rollen mit mehr als einer OneLogin Anwendung zu ermitteln

1. (Optional) Weisen Sie der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Ausnahmegenehmiger** die Identitäten zu, die über betroffene OneLogin Rollen informiert werden sollen und gegebenenfalls Ausnahmen genehmigen dürfen.
 1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Ausnahmegenehmiger**.
 2. Wählen Sie die Aufgabe **Identitäten zuweisen**.
 3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Identitäten zu.

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

Um eine Zuweisung zu entfernen

 - Wählen Sie die Identität und doppelklicken Sie .
 4. Speichern Sie die Änderungen.
2. (Optional) Prüfen Sie, ob Benachrichtigungen über Richtlinienverletzungen eingerichtet sind.

Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für Unternehmensrichtlinien*.
3. Aktivieren Sie die Arbeitskopie der Unternehmensrichtlinie **Allen OneLogin Rollen ist nur eine OneLogin Anwendung zugewiesen**.

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien > Vordefiniert**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Arbeitskopie aktivieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Aktivieren Sie die originale Richtlinie. Bestätigen Sie die Abfrage mit **Ja**.

Die Richtlinienprüfung wird anschließend gestartet.

TIPP: Wenn bereits eine aktive Unternehmensrichtlinie vorhanden ist, können Sie die Richtlinienprüfung über die Aufgabe **Richtlinie neu berechnen** starten.

Durch den hinterlegten Zeitplan wird die Richtlinienprüfung einmal monatlich gestartet.

4. Überprüfen Sie alle OneLogin Rollen, welche die Richtlinie verletzen und korrigieren Sie die Zuweisungen von OneLogin Anwendungen.

Um OneLogin Anwendung zu ermitteln, die mehr als einer OneLogin Rolle zugewiesen sind

1. (Optional) Weisen Sie der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Ausnahmegenehmiger** die Identitäten zu, die über betroffene Anwendungen informiert werden sollen und gegebenenfalls Ausnahmen genehmigen dürfen.

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Ausnahmegenehmiger**.
2. Wählen Sie die Aufgabe **Identitäten zuweisen**.
3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Identitäten zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Identität und doppelklicken Sie .

4. Speichern Sie die Änderungen.

2. (Optional) Prüfen Sie, ob Benachrichtigungen über Richtlinienverletzungen eingerichtet sind.

Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für Unternehmensrichtlinien*.

3. Aktivieren Sie die Arbeitskopie der Unternehmensrichtlinie **Alle OneLogin Anwendungen sind nur einer OneLogin Rolle zugewiesen**.

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien > Vordefiniert**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Arbeitskopie aktivieren**.

4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Aktivieren Sie die originale Richtlinie. Bestätigen Sie die Abfrage mit **Ja**.

Die Richtlinienprüfung wird anschließend gestartet.

TIPP: Wenn bereits eine aktive Unternehmensrichtlinie vorhanden ist, können Sie die Richtlinienprüfung über die Aufgabe **Richtlinie neu berechnen** starten.

Durch den hinterlegten Zeitplan wird die Richtlinienprüfung einmal monatlich gestartet.

4. Überprüfen Sie alle OneLogin Anwendungen, welche die Richtlinie verletzen und korrigieren Sie die Zuweisungen zu OneLogin Rollen.

Verwandte Themen

- [Behavior Driven Governance für OneLogin](#) auf Seite 6
- [Voraussetzungen für den automatischen Entzug ungenutzter OneLogin Anwendungen](#) auf Seite 7
- [Ungenutzte Zugänge zu OneLogin Anwendungen ermitteln](#) auf Seite 8
- [Ungenutzte OneLogin Anwendungen ermitteln](#) auf Seite 12

Behavior Driven Governance für Privileged Account Management

HINWEIS: Die Funktionalität steht zur Verfügung, wenn das Privileged Account Governance Modul installiert ist.

One Identity Manager stellt verschiedene Unternehmensrichtlinien und Attestierungsrichtlinien bereit, um Berechtigungen in One Identity Safeguard abhängig vom Nutzungsverhalten ihrer Benutzer zu überprüfen und zu rezertifizieren oder zu entfernen. Folgende Szenarien können damit behandelt werden:

- PAM Benutzergruppen, die von ihren Benutzern nicht genutzt werden

Die Mitglieder von Benutzergruppen sollten innerhalb eines definierten Zeitraums Zugriffsanforderungen stellen. Für Benutzerkonten, für die im PAM Prüfprotokoll keine Zugriffsanforderungen aufgezeichnet sind, soll die Mitgliedschaft in der Benutzergruppe rezertifiziert oder gelöscht werden.

Über eine Unternehmensrichtlinie werden alle Benutzerkonten ohne Zugriffsanforderungen ermittelt. Ausnahmegenehmiger werden über die betroffenen Benutzergruppen und Benutzerkonten informiert. Parallel dazu wird ein Rezertifizierungsverfahren gestartet. Im Lauf der Rezertifizierung erklären die Entscheider der Attestierungsrichtlinie, ob die Mitgliedschaften weiterhin benötigt werden. Nicht benötigte Mitgliedschaften können anschließend automatisch oder manuell entfernt werden.

- Verschiedene PAM Berechtigungen, die nicht genutzt werden

PAM Berechtigungen, wie Assets, Benutzergruppen oder Nutzungsrechte, sollten mindestens einmal innerhalb eines definierten Zeitraums genutzt werden. Wenn eine Berechtigung laut PAM Prüfprotokoll in diesem Zeitraum nicht genutzt wurde, kann in einem Rezertifizierungsverfahren entschieden werden, ob die Berechtigung weiterhin benötigt wird.

Über verschiedene Unternehmensrichtlinie werden alle ungenutzten Berechtigungen ermittelt. Ausnahmegenehmiger werden über die betroffenen Berechtigungen informiert. Über eine Rezertifizierung kann geklärt werden, ob die Berechtigungen noch benötigt werden. Ungenutzte Berechtigungen können anschließend im Zielsystem entfernt werden.

Nach welchem Zeitraum Berechtigungen als ungenutzt betrachtet werden, ist im Konfigurationsparameter **TargetSystem | PAG | UnusedThresholdInDays** festgelegt. Der Standardwert ist 90 Tage.

Ausführliche Informationen zur Abbildung von PAM-Objekten finden Sie im *One Identity Manager Administrationshandbuch für die Privileged Account Governance*.

Verwandte Themen

- [Behavior Driven Governance für Zielsysteme im Unified Namespace](#) auf Seite 21
- [Behavior Driven Governance für OneLogin](#) auf Seite 6

Behavior Driven Governance für Zielsysteme im Unified Namespace

One Identity Manager stellt Unternehmensrichtlinien bereit, um Benutzerkonten zu ermitteln, die für einen definierten Zeitraum nicht genutzt wurden. Mit diesen Informationen können Administratoren die Zugangsberechtigungen zu den Zielsystemen überprüfen und korrigieren. Sicherheitsrisiken, die mit ungenutzten, aber aktiven Benutzerkonten verbunden sind, können so verringert werden.

Voraussetzungen

- Die Benutzerkonten sind im Unified Namespace abgebildet.
- Die Zielsysteme stellen eine Information über die Nutzungsdauer der Benutzerkonten bereit. Diese Daten werden mit One Identity Manager synchronisiert und in UNSAccount.LastLogon abgebildet.

Ausführliche Informationen zur Abbildung von Zielsystemen und Benutzerkonten im Unified Namespace finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Nach welchem Zeitraum Benutzerkonten als ungenutzt betrachtet werden, ist im Konfigurationsparameter **TargetSystem | UNS | UnusedUserAccountThresholdInDays** festgelegt. Der Standardwert ist 90 Tage.

Folgende Szenarien können behandelt werden:

- Benutzerkonten, die nicht genutzt werden, können deaktiviert werden
Wenn Benutzer sich innerhalb eines definierten Zeitraums nicht am Zielsystem angemeldet haben, kann deren Benutzerkonto als ungenutzt betrachtet werden. Solche Benutzerkonten sollten deaktiviert werden, damit keine Anmeldung mehr möglich ist.
- Benutzerkonten, die nicht genutzt werden, können gelöscht werden
Benutzerkonten, die innerhalb eines definierten Zeitraums nicht zur Anmeldung am Zielsystem genutzt wurden, sollten gelöscht werden.

Mit den Standard-Unternehmensrichtlinien können ungenutzte Benutzerkonten ermittelt und die Ausnahmegenehmiger informiert werden. Wie mit diesen Benutzerkonten

verfahren werden soll (deaktivieren oder löschen), ist von den Möglichkeiten der jeweiligen Zielsysteme abhängig. Definieren Sie dafür zielsystemspezifische Prozesse.

Detaillierte Informationen zum Thema

- [Ungenutzte Benutzerkonten ermitteln und deaktivieren](#) auf Seite 22
- [Ungenutzte Benutzerkonten ermitteln und löschen](#) auf Seite 23

Verwandte Themen

- [Behavior Driven Governance für OneLogin](#) auf Seite 6

Ungenutzte Benutzerkonten ermitteln und deaktivieren

Ob ungenutzte Benutzerkonten automatisiert oder manuell deaktiviert werden können, ist abhängig von den Möglichkeiten der jeweiligen Zielsysteme und Ihren unternehmensspezifischen IT-Richtlinien. Definieren Sie geeignete Prozesse, um Administratoren, Manager oder andere Verantwortliche über ungenutzte Benutzerkonten zu informieren und die betroffenen Benutzerkonten zu deaktivieren.

Um ungenutzte Benutzerkonten zu ermitteln und zu deaktivieren

1. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | UNS | UnusedUserAccountThresholdInDays | DaysUntilDisable** und erfassen Sie als Wert die Anzahl der Tage, nach denen ungenutzte Benutzerkonten deaktiviert werden sollen. Der Standardwert ist 180 Tage.
2. (Optional) Weisen Sie der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Ausnahmegenehmiger** die Identitäten zu, die über betroffene Benutzerkonten informiert werden sollen und gegebenenfalls Ausnahmen genehmigen dürfen.

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Ausnahmegenehmiger**.
2. Wählen Sie die Aufgabe **Identitäten zuweisen**.
3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Identitäten zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Identität und doppelklicken Sie .
4. Speichern Sie die Änderungen.

3. (Optional) Prüfen Sie, ob Benachrichtigungen über Richtlinienverletzungen eingerichtet sind.

Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für Unternehmensrichtlinien*.

4. Aktivieren Sie die Arbeitskopie der Unternehmensrichtlinie **Ungenutzte Benutzerkonten können deaktiviert werden**.
 1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien > Vordefiniert**.
 2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
 3. Wählen Sie die Aufgabe **Arbeitskopie aktivieren**.
 4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
 5. Aktivieren Sie die originale Richtlinie. Bestätigen Sie die Abfrage mit **Ja**.

Die Richtlinienprüfung wird anschließend gestartet.

TIPP: Wenn bereits eine aktive Unternehmensrichtlinie vorhanden ist, können Sie die Richtlinienprüfung über die Aufgabe **Richtlinie neu berechnen** starten.

Durch den hinterlegten Zeitplan wird die Richtlinienprüfung einmal monatlich gestartet.

5. Überprüfen Sie alle Benutzerkonten, welche die Richtlinie verletzen und deaktivieren Sie diese.
 - Um die ungenutzten Benutzerkonten automatisch zu deaktivieren, erstellen Sie zielsystemspezifische Prozesse, die bei neuen Richtlinienverletzungen ausgeführt werden.

Verwandte Themen

- [Behavior Driven Governance für Zielsysteme im Unified Namespace](#) auf Seite 21
- [Ungenutzte Benutzerkonten ermitteln und löschen](#) auf Seite 23

Ungenutzte Benutzerkonten ermitteln und löschen

Ob ungenutzte Benutzerkonten automatisiert oder manuell gelöscht werden können, ist abhängig von den Möglichkeiten der jeweiligen Zielsysteme und Ihren unternehmensspezifischen IT-Richtlinien. Definieren Sie geeignete Prozesse, um Administratoren, Manager oder andere Verantwortliche über ungenutzte Benutzerkonten zu informieren und die betroffenen Benutzerkonten zu löschen.

Um ungenutzte Benutzerkonten zu ermitteln und zu löschen

1. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | UNS | UnusedUserAccountThresholdInDays | DaysUntilDelete** und erfassen Sie als Wert die Anzahl der Tage, nach denen ungenutzte Benutzerkonten deaktiviert werden sollen. Der Standardwert ist 360 Tage.
2. (Optional) Weisen Sie der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Ausnahmegenehmiger** die Identitäten zu, die über betroffene Benutzerkonten informiert werden sollen und gegebenenfalls Ausnahmen genehmigen dürfen.

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Ausnahmegenehmiger**.
2. Wählen Sie die Aufgabe **Identitäten zuweisen**.
3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Identitäten zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Identität und doppelklicken Sie .
4. Speichern Sie die Änderungen.
 3. (Optional) Prüfen Sie, ob Benachrichtigungen über Richtlinienverletzungen eingerichtet sind.

Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für Unternehmensrichtlinien*.

4. Aktivieren Sie die Arbeitskopie der Unternehmensrichtlinie **Ungenutzte Benutzerkonten können gelöscht werden**.
 1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien > Vordefiniert**.
 2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
 3. Wählen Sie die Aufgabe **Arbeitskopie aktivieren**.
 4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
 5. Aktivieren Sie die originale Richtlinie. Bestätigen Sie die Abfrage mit **Ja**.

Die Richtlinienprüfung wird anschließend gestartet.

TIPP: Wenn bereits eine aktive Unternehmensrichtlinie vorhanden ist, können Sie die Richtlinienprüfung über die Aufgabe **Richtlinie neu berechnen** starten.

Durch den hinterlegten Zeitplan wird die Richtlinienprüfung einmal monatlich gestartet.

5. Überprüfen Sie alle Benutzerkonten, welche die Richtlinie verletzen und löschen Sie diese.
 - Um die ungenutzten Benutzerkonten automatisch zu löschen, erstellen Sie

zielsystemspezifische Prozesse, die bei neuen Richtlinienverletzungen ausgeführt werden.

Verwandte Themen

- [Behavior Driven Governance für Zielsysteme im Unified Namespace](#) auf Seite 21
- [Ungenutzte Benutzerkonten ermitteln und deaktivieren](#) auf Seite 22

Konfigurationsparameter für Behavior Driven Governance

Für Behavior Driven Governance sind folgende Konfigurationsparameter relevant.

Tabelle 1: Übersicht der Konfigurationsparameter für Behavior Driven Governance

Konfigurationsparameter	Beschreibung
TargetSystem OneLogin UnusedApplicationThresholdInDays	Anzahl an Tagen, nach denen der Zugang zu einer OneLogin Anwendung als ungenutzt betrachtet wird (Standard: 90).
TargetSystem PAG UnusedThresholdInDays	Anzahl der Tage, nach denen ein privilegiertes Objekt, eine Berechtigung oder ein Benutzer als ungenutzt gilt (Standard: 90).
TargetSystem UNS UnusedUserAccountThresholdInDays	Anzahl der Tage, nach denen ein Benutzerkonto als ungenutzt betrachtet wird (Standard: 90).
TargetSystem UNS UnusedUserAccountThresholdInDays DaysUntilDelete	Anzahl der Tage, nach denen ein ungenutztes Benutzerkonto gelöscht werden soll (Standard: 365).
TargetSystem UNS UnusedUserAccountThresholdInDays DaysUntilDisable	Anzahl der Tage, nach denen ein ungenutztes Benutzerkonto deaktiviert werden soll (Standard: 180).
QER Attestation AutoRemovalScope und alle untergeordneten Konfigurationsparameter	Allgemeiner Konfigurationsparameter zur Definition des automatischen Entzugs von Berechtigungen nach einer negativen Entscheidung im Rahmen einer Attestierung.

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

B

- Behavior Driven Governance 4
 - Benutzerkonten im Unified Namespace 21
 - OneLogin 6
 - Privileged Account Management 19
 - ungenutzte Anwendungen 8, 12
 - ungenutzte Benutzerkonten 22-23
 - vorbereiten 7, 16

O

- OneLogin
 - Behavior Driven Governance 6
 - ungenutzte Anwendungen 12
 - ungenutzte Anwendungen entfernen 7
 - ungenutzte Zugänge zu Anwendungen entfernen 8, 12
 - Zuweisung von Anwendungen an Rollen prüfen 16

P

- Privileged Account Management
 - Behavior Driven Governance 19

U

- Unified Namespace
 - Behavior Driven Governance 21
 - ungenutzte Benutzerkonten deaktivieren 22
 - ungenutzte Benutzerkonten löschen 23