



One Identity Manager 9.3

Administrationshandbuch für
Unternehmensrichtlinien

Copyright 2025 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 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 Unternehmensrichtlinien
Aktualisiert - 06. Januar 2025, 12:20 Uhr

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

Inhalt

Unternehmensrichtlinien im One Identity Manager	6
One Identity Manager Benutzer für Unternehmensrichtlinien	7
Definieren von Unternehmensrichtlinien	11
Unternehmensrichtlinien erstellen und bearbeiten	11
Allgemeine Stammdaten für Unternehmensrichtlinien	12
Risikobewertung für Richtlinienverletzungen	15
Erweiterte Angaben für Unternehmensrichtlinien	17
Arbeitskopien und Originale von Unternehmensrichtlinien vergleichen	18
Zusätzliche Aufgaben für Arbeitskopien von Unternehmensrichtlinien	19
Arbeitskopien von Unternehmensrichtlinien aktivieren	19
Arbeitskopien von Unternehmensrichtlinien kopieren	19
Bedingungen von Arbeitskopien von Unternehmensrichtlinien anzeigen	20
Ausgewählte Objekte für Arbeitskopien anzeigen	20
Ausnahmegenehmiger für Arbeitskopien pflegen	21
Richtlinienverantwortliche für Arbeitskopien pflegen	22
Compliance Frameworks an Arbeitskopien von Unternehmensrichtlinien zuweisen	22
Risikomindernde Maßnahmen an Arbeitskopien zuweisen	23
Überblick über Arbeitskopien anzeigen	23
Zusätzliche Aufgaben für Unternehmensrichtlinien	24
Unternehmensrichtlinien aktivieren und deaktivieren	24
Arbeitskopien für Unternehmensrichtlinien erstellen	25
Unternehmensrichtlinien kopieren	25
Bedingungen von Unternehmensrichtlinien anzeigen	26
Ausgewählte Objekte für Unternehmensrichtlinien anzeigen	26
Ausnahmegenehmiger für Unternehmensrichtlinien pflegen	27
Richtlinienverantwortliche für Unternehmensrichtlinien pflegen	27
Attestierungsvorgänge erstellen	28
Überblick über Unternehmensrichtlinien anzeigen	29
Standard-Unternehmensrichtlinien verwenden	29
Unternehmensrichtlinien löschen	30
Richtliniengruppen	30

Compliance Frameworks	31
Compliance Frameworks an Unternehmensrichtlinien zuweisen	32
Überblick über Compliance Frameworks anzeigen	33
Zeitpläne für die Richtlinienprüfung	33
Unternehmensrichtlinien an Zeitpläne zuweisen	37
Zeitpläne sofort ausführen	38
Überblick über Zeitpläne anzeigen	38
Attestierer für Unternehmensrichtlinien	38
Richtlinienverantwortliche für Unternehmensrichtlinien	39
Ausnahmegenehmiger für Richtlinienverletzungen	41
Standardbegründungen für Richtlinienverletzungen	42
Vordefinierte Standardbegründungen für Richtlinienverletzungen	43
Mailvorlagen für Benachrichtigungen über Unternehmensrichtlinien	43
Maildefinitionen für Unternehmensrichtlinien erstellen und bearbeiten	44
Basisobjekte für Mailvorlagen für Unternehmensrichtlinien	45
Mailvorlagen für Unternehmensrichtlinien bearbeiten	45
Verwenden von Hyperlinks zum Web Portal	47
Standardfunktionen für die Erstellung von Hyperlinks	48
Überprüfen der Unternehmensrichtlinien	49
Berechnen von Richtlinienverletzungen	49
Zeitgesteuerte Richtlinienprüfung	50
Ad-hoc-Richtlinienprüfung	50
Berichte über Richtlinienverletzungen	51
Erteilen von Ausnahmegenehmigungen	51
Benachrichtigungen über Richtlinienverletzungen	52
Aufforderung zur Ausnahmegenehmigung	53
Benachrichtigung über Richtlinienverletzungen ohne Ausnahmegenehmigung	54
Entscheidungsstatus von Richtlinienverletzungen anzeigen	55
Automatische Attestierung von Richtlinienverletzungen	56
Automatische Attestierung von Richtlinienverletzungen konfigurieren	56
Attestierung von Richtlinienverletzungen starten	57
Fehler bei der Attestierung von Richtlinienverletzungen	58
Risikomindernde Maßnahmen für Unternehmensrichtlinien	60
Risikomindernde Maßnahmen für Unternehmensrichtlinien erstellen und bearbeiten	61

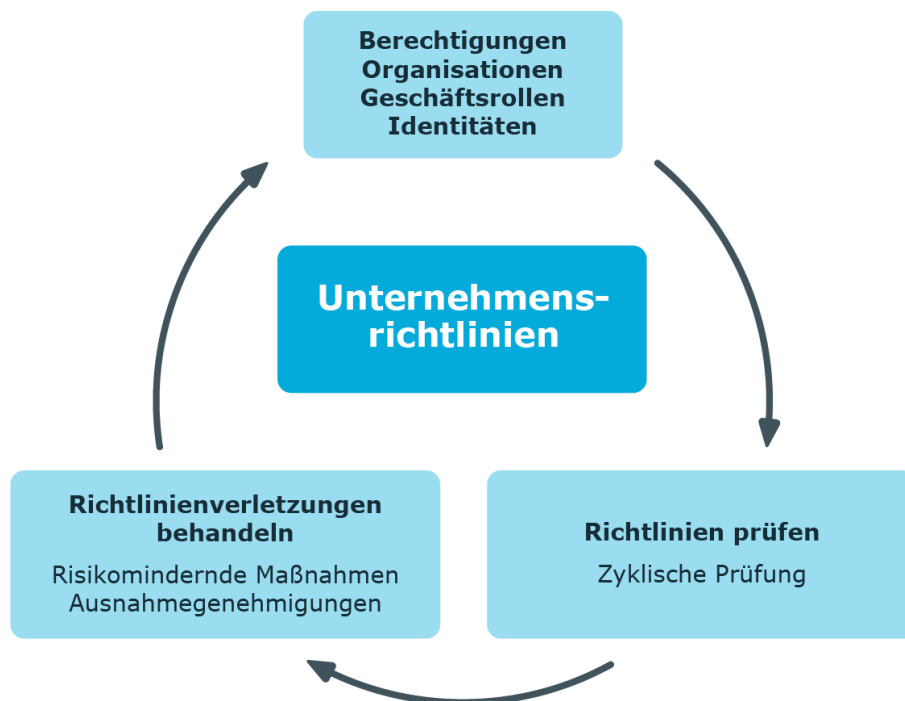
Unternehmensrichtlinien an risikomindernde Maßnahmen zuweisen	61
Risikominderung für Unternehmensrichtlinien berechnen	62
Überblick über risikomindernde Maßnahmen für Unternehmensrichtlinien anzeigen	62
Anhang: Konfigurationsparameter für Unternehmensrichtlinien	64
Über uns	66
Kontaktieren Sie uns	66
Technische Supportressourcen	66
Index	67

Unternehmensrichtlinien im One Identity Manager

Unternehmen haben unterschiedlichste Anforderungen, durch die der Zugriff für interne und externe Mitarbeiter auf die Unternehmensressourcen reguliert werden soll. Zusätzlich muss nachgewiesen werden, dass Anforderungen der Gesetzgeber eingehalten werden. Derartige Anforderungen können als Richtlinien definiert werden.

Der One Identity Manager bietet die Möglichkeit, diese Unternehmensrichtlinien zu verwalten und die damit verbundenen Risiken zu bewerten. Soweit die entsprechenden Daten in der One Identity Manager-Datenbank hinterlegt sind, ermittelt der One Identity Manager alle Unternehmensressourcen, die diese Unternehmensrichtlinien verletzen. Zu Berichtszwecken können auch Unternehmensrichtlinien definiert werden, die keinen Bezug zum Datenmodell des One Identity Manager haben.

Abbildung 1: Unternehmensrichtlinien im One Identity Manager



Über zeitgesteuerte Aufträge wird die Einhaltung der Unternehmensrichtlinien regelmäßig überprüft. Um den weiteren Umgang mit verletzten Unternehmensrichtlinien zu bestimmen, beziehen Sie diese in die regelmäßige Attestierung Ihrer Unternehmensressourcen ein. Für alle Unternehmensrichtlinien kann eine Risikobewertung durchgeführt werden. Verschiedene Berichte und Statistiken verschaffen Ihnen einen Überblick über die verletzten Richtlinien.

Beispiele für Unternehmensrichtlinien sind:

- Allen Kostenstellen ist ein Manager zugeordnet.
- Allen Abteilungen sind Identitäten zugewiesen.
- Alle Identitäten sind attestiert.
- Deaktivierte Identitäten besitzen keine aktivierten Benutzerkonten.

HINWEIS: Voraussetzung für die Nutzung von Unternehmensrichtlinien im One Identity Manager ist die Installation des Modul Unternehmensrichtlinien. Ausführliche Informationen zur Installation finden Sie im *One Identity Manager Installationshandbuch*.

Um Unternehmensrichtlinien abbilden zu können

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Policy**.

Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL-Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.

One Identity Manager Benutzer für Unternehmensrichtlinien

In die Verwaltung von Unternehmensrichtlinien sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Administratoren für Unternehmensrichtlinien	Die Administratoren müssen der Anwendungsrolle Identity & Access Governance Unternehmensrichtlinien Administratoren zugewiesen sein. Benutzer mit dieser Anwendungsrolle: <ul style="list-style-type: none">• Erstellen die Basisdaten für die Erstellung der Unternehmensrichtlinien.• Erstellen die Richtlinien und weisen die

Benutzer

Aufgaben

Benutzer	Aufgaben
	<p>Richtlinienverantwortlichen zu.</p> <ul style="list-style-type: none">• Können bei Bedarf die Berechnung der Richtlinien starten und Richtlinienverletzungen einsehen.• Erstellen Berichte über Richtlinienverletzungen.• Erfassen risikomindernde Maßnahmen.• Erstellen und bearbeiten Risikoindex-Berechnungsvorschriften.• Administrieren die Anwendungsrollen für Richtlinienverantwortliche, Ausnahmegenehmiger und Attestierer.• Richten bei Bedarf weitere Anwendungsrollen ein.
Richtlinienverantwortliche	<p>Die Richtlinienverantwortlichen müssen der Anwendungsrolle Identity & Access Governance Unternehmensrichtlinien Richtlinienverantwortliche oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Sind inhaltlich verantwortlich für Unternehmensrichtlinien.• Bearbeiten die Arbeitskopien der Unternehmensrichtlinien.• Aktivieren und deaktivieren Unternehmensrichtlinien.• Können bei Bedarf die Berechnung der Richtlinien starten und Richtlinienverletzungen einsehen.• Weisen risikomindernde Maßnahmen zu.
One Identity Manager Administratoren	<p>One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen.</p> <p>One Identity Manager Administratoren:</p> <ul style="list-style-type: none">• 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.

Benutzer	Aufgaben
Ausnahmegenehmiger	<ul style="list-style-type: none"> • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. <p>Die Ausnahmegenehmiger müssen der Anwendungsrolle Identity & Access Governance Unternehmensrichtlinien Ausnahmegenehmiger oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Bearbeiten die Richtlinienverletzungen. • Können Ausnahmegenehmigungen erteilen oder entziehen.
Attestierer für Unternehmensrichtlinien	<p>Die Attestierer müssen der Anwendungsrolle Identity & Access Governance Unternehmensrichtlinien Attestierer zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Attestieren im Web Portal die Unternehmensrichtlinien und Ausnahmegenehmigungen, für die sie verantwortlich sind. • Können die Stammdaten der Unternehmensrichtlinien sehen, aber nicht bearbeiten.
Compliance & Security Officer	<p>Compliance & Security Officer müssen der Anwendungsrolle Identity & Access Governance Compliance & Security Officer zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Sehen im Web Portal alle Compliance-relevanten Informationen und deren Auswertungen. Dazu gehören Attestierungsrichtlinien, Unternehmensrichtlinien und Richtlinienverletzungen, Complianceregelungen und Regelverletzungen sowie Risikoindex-Berechnungsvorschriften. • Können Attestierungsrichtlinien bearbeiten.
Auditoren	<p>Die Auditoren sind der Anwendungsrolle Identity &</p>

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

Benutzer

Aufgaben

Access Governance | Auditoren zugewiesen.

Benutzer mit dieser Anwendungsrolle:

- Sehen im Web Portal alle für ein Audit relevanten Daten.

Definieren von Unternehmensrichtlinien

Unternehmensrichtlinien beinhalten im One Identity Manager neben der technischen Beschreibung auch weitere Eigenschaften, wie beispielsweise Risikobewertung einer Richtlinienverletzung und Verantwortlichkeiten. Ebenso ist eine Klassifizierung der Unternehmensrichtlinien nach Compliance Frameworks und eine Strukturierung in Richtliniengruppen möglich.

Detaillierte Informationen zum Thema


- [Standard-Unternehmensrichtlinien verwenden](#) auf Seite 29
- [Unternehmensrichtlinien erstellen und bearbeiten](#) auf Seite 11
- [Unternehmensrichtlinien löschen](#) auf Seite 30

Unternehmensrichtlinien erstellen und bearbeiten

Für jede Unternehmensrichtlinie wird in der Datenbank eine Arbeitskopie angelegt. Um Unternehmensrichtlinien zu erstellen und zu ändern, bearbeiten Sie deren Arbeitskopie. Erst mit Aktivierung der Arbeitskopie werden die Änderungen auf die Unternehmensrichtlinie übertragen.

HINWEIS: One Identity Manager Benutzer mit der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Richtlinienverantwortliche** können bestehende Unternehmensrichtlinien bearbeiten, für die sie als Verantwortliche in den Stammdaten eingetragen sind.

Um eine neue Unternehmensrichtlinie zu erstellen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Klicken Sie in der Ergebnisliste .
3. Erfassen Sie die Stammdaten der Unternehmensrichtlinie.

4. Speichern Sie die Änderungen.
Es wird eine Arbeitskopie angelegt.
5. Wählen Sie die Aufgabe **Arbeitskopie aktivieren**. Bestätigen Sie die Sicherheitsabfrage mit **OK**.
Es wird eine aktive Unternehmensrichtlinie angelegt. Die Arbeitskopie bleibt bestehen und wird für nachfolgende Änderungen genutzt.

Um eine bestehende Unternehmensrichtlinie zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
 - a. Wählen Sie in der Ergebnisliste eine Unternehmensrichtlinie.
 - b. Wählen Sie die Aufgabe **Arbeitskopie erstellen**.
Die Daten der bestehenden Arbeitskopie werden auf Nachfrage mit den Daten der originalen Unternehmensrichtlinie überschrieben. Die Arbeitskopie wird geöffnet und kann bearbeitet werden.
- ODER -
- Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien**.
 - a. Wählen Sie in der Ergebnisliste eine Arbeitskopie.
 - b. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
2. Bearbeiten Sie die Stammdaten der Arbeitskopie.
3. Speichern Sie die Änderungen.
4. Wählen Sie die Aufgabe **Arbeitskopie aktivieren**. Bestätigen Sie die Sicherheitsabfrage mit **OK**.
Die Änderungen an der Arbeitskopie werden auf die Unternehmensrichtlinie übertragen. Dabei wird eine deaktivierte Unternehmensrichtlinien auf Nachfrage aktiviert.



Allgemeine Stammdaten für Unternehmensrichtlinien

Für eine Unternehmensrichtlinie erfassen Sie die folgenden Stammdaten.

Tabelle 2: Allgemeine Stammdaten einer Unternehmensrichtlinie

Eigenschaft	Beschreibung
Richtlinie	Bezeichnung der Unternehmensrichtlinie.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Hauptversionsnummer	Bearbeitungsstand der Unternehmensrichtlinie als Versi-

Eigenschaft	Beschreibung
	onsnummern. Bei jeder Änderung der Bedingung wird in der Standardinstallation des One Identity Manager die letzte Stelle der Versionsnummer erhöht.
Arbeitskopie	Gibt an, ob es sich um die Arbeitskopie der Unternehmensrichtlinie handelt.
Deaktiviert	Gibt an, ob die Unternehmensrichtlinie deaktiviert ist. Nur aktivierte Unternehmensrichtlinien werden bei der Richtlinienprüfung berücksichtigt. Zur Aktivierung und Deaktivierung einer Unternehmensrichtlinie verwenden Sie die Aufgaben Richtlinie aktivieren und Richtlinie deaktivieren . Die Arbeitskopie einer Unternehmensrichtlinie ist immer deaktiviert.
Richtliniengruppe	Richtliniengruppe, zu der die Unternehmensrichtlinie inhaltlich gehört. Wählen Sie eine Richtliniengruppe aus der Auswahlliste aus. Um eine neue Richtliniengruppe zu erstellen, klicken Sie  . Erfassen Sie den Namen und eine Beschreibung der Richtliniengruppe.
Richtlinienverantwortliche	Anwendungsrolle, deren Mitglieder inhaltlich für die Unternehmensrichtlinie verantwortlich sind. Um eine neue Anwendungsrolle zu erstellen, klicken Sie  . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Ausnahmegenehmigung möglich	Gibt an, ob Ausnahmegenehmigungen erlaubt sind, wenn die Unternehmensrichtlinie verletzt wird. Zuweisungen, die eine Richtlinienverletzung verursachen, können somit trotzdem genehmigt und zugewiesen werden.
Attestierungsrichtlinie	Attestierungsrichtlinie, die für die Attestierung von Objekten genutzt werden soll, welche diese Unternehmensrichtlinie verletzen. WICHTIG: Stellen Sie sicher, dass durch diese Attestierungsrichtlinie die gleichen Objekte ermittelt werden, wie durch die Unternehmensrichtlinie. Prüfen Sie die zugeordneten Tabellen und Bedingungen. Dieses Feld wird nur angezeigt, wenn das Modul Attestierung installiert ist. Diese Funktionalität wird standardmäßig im Rahmen des Behavior Driven Governance genutzt. Ausführliche Informationen dazu finden Sie im <i>One Identity Manager Administrationshandbuch für Behavior Driven Governance</i> .

Eigenschaft	Beschreibung
Attestierung für neue Richtlinienverletzungen sofort starten	<p>Gibt an, ob für jede neue Richtlinienverletzung sofort ein Attestierungsvorgang erstellt werden soll. Wenn Sie diese Option aktivieren, ordnen Sie eine Attestierungsrichtlinie zu.</p> <p>Dieses Feld wird nur angezeigt, wenn das Modul Attestierung installiert ist.</p> <p>Diese Funktionalität wird standardmäßig im Rahmen des Behavior Driven Governance genutzt. Ausführliche Informationen dazu finden Sie im <i>One Identity Manager Administrationshandbuch für Behavior Driven Governance</i>.</p>
Ausnahmegenehmiger	<p>Anwendungsrolle, deren Mitglieder berechtigt sind, Ausnahmegenehmigungen für Verletzungen dieser Unternehmensrichtlinie zu erteilen.</p> <p>Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.</p>
Mailvorlage neue Verletzung	<p>Mailvorlage, die zur Generierung einer E-Mail verwendet wird, um Richtlinienverantwortliche oder Ausnahmegenehmiger über neue Richtlinienverletzungen zu informieren.</p>
Hinweise zur Ausnahmegenehmigung	<p>Informationen, die Ausnahmegenehmiger für ihre Entscheidung benötigen. Diese Hinweise sollten die Risiken und Nebenwirkungen einer Ausnahmegenehmigung beschreiben.</p>
Attestierer	<p>Anwendungsrolle, deren Mitglieder berechtigt sind, Attestierungsvorgänge über Unternehmensrichtlinien und Richtlinienverletzungen zu entscheiden.</p> <p>Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.</p>
Ohne Bedingung	<p>Gibt an, ob die Unternehmensrichtlinie keinen direkten Bezug zum One Identity Manager-Datenmodell hat. Wenn die Option aktiviert ist, wird die Schaltfläche Bedingung bearbeiten... deaktiviert.</p> <p>Wenn die Option deaktiviert ist, muss eine Bedingung formuliert werden, die alle Objekte ermittelt, welche die Unternehmensrichtlinie verletzen.</p>
Basistabelle	<p>Basistabelle, auf die sich die Unternehmensrichtlinie bezieht.</p> <p>Ausgehend von dieser Tabelle, werden die Objekte</p>

Eigenschaft	Beschreibung
	ermittelt, welche die Unternehmensrichtlinie verletzen.
Bedingung bearbeiten...	Startet den Where-Klausel-Assistenten. Mit dem Where-Klausel-Assistenten können Sie eine Bedingung erstellen, die alle Objekte aus der Basistabelle ermittelt, welche die Unternehmensrichtlinie verletzen. Über die Schaltfläche Expertenansicht wechseln Sie zur direkten Eingabe der Bedingung in SQL-Syntax.
Bedingung	Datenbankabfrage, über welche die Objekte ermittelt werden, die die Unternehmensrichtlinie verletzen. Das Eingabefeld ist nur sichtbar, wenn zuvor die Aufgabe Bedingung anzeigen ausgeführt wurde.

Detaillierte Informationen zum Thema

- [Unternehmensrichtlinien aktivieren und deaktivieren](#) auf Seite 24
- [Richtliniengruppen](#) auf Seite 30
- [Richtlinienverantwortliche für Unternehmensrichtlinien](#) auf Seite 39
- [Ausnahmegenehmiger für Richtlinienverletzungen](#) auf Seite 41
- [Attestierer für Unternehmensrichtlinien](#) auf Seite 38
- [Bedingungen von Arbeitskopien von Unternehmensrichtlinien anzeigen](#) auf Seite 20
- [Automatische Attestierung von Richtlinienverletzungen konfigurieren](#) auf Seite 56

Verwandte Themen

- [Benachrichtigung über Richtlinienverletzungen ohne Ausnahmegenehmigung](#) auf Seite 54
- [Aufforderung zur Ausnahmegenehmigung](#) auf Seite 53

Risikobewertung für Richtlinienverletzungen

Ausführliche Informationen zur Risikobewertung finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.

Mit dem One Identity Manager können Sie die Risiken von Richtlinienverletzungen bewerten. Dazu legen Sie an den Unternehmensrichtlinien einen Risikoindex fest. Der Risikoindex gibt an, welches Risiko für Ihr Unternehmen besteht, wenn die Unternehmensrichtlinie verletzt wird. Der Risikoindex wird als numerischer Wert mit dem Wertebereich 0 ... 1 angegeben. Dabei legen Sie fest, ob mit einer Richtlinienverletzung für Ihr Unternehmen kein Risiko verbunden ist (Risikoindex = 0) oder ob jede Richtlinienverletzung ein Problem darstellt (Risikoindex = 1).

Um Richtlinienverletzungen abhängig vom Risikoindex auszuwerten, können Sie mit dem Report Editor verschiedene Berichte erstellen. Ausführliche Informationen zum Erstellen von Berichten finden Sie im *One Identity Manager Konfigurationshandbuch*.

Für die Risikobewertung einer Richtlinienverletzung erfassen Sie auf dem Tabreiter **Bewertungskriterien** Werte für die Einstufung der Unternehmensrichtlinie.

Tabelle 3: Bewertungskriterien einer Regel

Eigenschaft	Beschreibung
Schweregrad	Gibt an, welche Auswirkung Verletzungen dieser Unternehmensrichtlinie für das Unternehmen haben. Stellen Sie über den Schieberegler einen Wert zwischen 0 und 1 ein. 0 ... keine Auswirkung 1 ... Jede Richtlinienverletzung ist ein Problem.
Auswirkung	Gibt in verbaler Beschreibung an, welche Auswirkung Verletzungen dieser Unternehmensrichtlinien für das Unternehmen haben. In der Standardinstallation werden die Werte Niedrig , Mittel , Hoch und Kritisch angezeigt.
Risikoindex	Gibt an, wie riskant Verletzungen dieser Unternehmensrichtlinien für das Unternehmen sind. Stellen Sie über den Schieberegler einen Wert zwischen 0 und 1 ein. 0 ... kein Risiko 1 ... Jede Regelverletzung ist ein Problem. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter QER CalculateRiskIndex aktiviert ist.
Risikoindex (reduziert)	Gibt den Risikoindex unter Berücksichtigung der zugewiesenen risikomindernden Maßnahmen an. Der Risikoindex einer Unternehmensrichtlinie wird um die Signifikanzminderung aller zugewiesenen risikomindernden Maßnahmen reduziert. Der Risikoindex (reduziert) wird nur für die originale Unternehmensrichtlinie berechnet. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter QER CalculateRiskIndex aktiviert ist und die originale Unternehmensrichtlinie angezeigt wird. Für Arbeitskopien wird das Feld nicht angezeigt. Der Wert wird durch den One Identity Manager berechnet und kann nicht bearbeitet werden.
Transparenzindex	Gibt an, wie nachvollziehbar Zuweisungen sind, die durch die Unternehmensrichtlinie geprüft werden. Stellen Sie über den Schieberegler einen Wert zwischen 0 und 1 ein. 0 ... keine Transparenz 1 ... volle Transparenz

Eigenschaft	Beschreibung
Max. Anzahl Regelverletzungen	Anzahl der Richtlinienverletzungen, die für diese Unternehmensrichtlinie zugelassen sind.

Detaillierte Informationen zum Thema

- [Risikomindernde Maßnahmen für Unternehmensrichtlinien](#) auf Seite 60

Verwandte Themen

- [Arbeitskopien für Unternehmensrichtlinien erstellen](#) auf Seite 25

Erweiterte Angaben für Unternehmensrichtlinien

Auf dem Tabreiter **Erweitert** erfassen Sie zusätzliche Anmerkungen zur Unternehmensrichtlinie.

Tabelle 4: Erweiterte Stammdaten einer Unternehmensrichtlinie

Eigenschaft	Beschreibung
Nummer der Richtlinie	Zusätzliche Bezeichnung der Unternehmensrichtlinie.
Anmerkungen zur Implementierung	Freitextfeld für zusätzliche Erläuterungen. Die Anmerkungen zur Implementierung können beispielsweise inhaltliche Erläuterungen zur Basistabelle und Richtlinienbedingung umfassen.
Status	Status der Unternehmensrichtlinie bezüglich ihres Revisionsstandes.
Zeitplan	Zeitplan, durch den die regelmäßige Überprüfung der Unternehmensrichtlinie gestartet wird. Standardmäßig ist der Zeitplan Richtlinienprüfung zugeordnet. Sie können hier einen eigenen Zeitplan zuordnen.

Verwandte Themen

- [Berechnen von Richtlinienverletzungen](#) auf Seite 49
- [Zeitpläne für die Richtlinienprüfung](#) auf Seite 33

Arbeitskopien und Originale von Unternehmensrichtlinien vergleichen

Wenn Sie die Bedingung der Unternehmensrichtlinie in einer Arbeitskopie geändert haben, können Sie die Auswirkungen dieser Änderung über einen Vergleich mit der originalen Unternehmensrichtlinie ermitteln. Unternehmensrichtlinien lassen sich nur vergleichen, wenn zu einer Arbeitskopie eine originale Unternehmensrichtlinie vorhanden ist.

TIPP: In der Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien > Geänderte Arbeitskopien** werden alle Arbeitskopien angezeigt, deren Bedingung nicht identisch ist mit der Bedingung der originalen Unternehmensrichtlinie.

Um eine Unternehmensrichtlinie mit der Arbeitskopie zu vergleichen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Richtlinienvergleich**.

Auf dem Tabreiter **Richtlinienvergleich** des Stammdatenformulars der Arbeitskopie werden daraufhin die Vergleichswerte dargestellt.

Tabelle 5: Ergebnis des Richtlinienvergleichs

Richtlinienverletzungen	Es werden alle Identitäten aufgelistet, die aufgrund der Änderung, die Unternehmensrichtlinie
Neu enthalten	erstmalig verletzen würden.
Identisch	weiterhin verletzen würden.
Nicht mehr enthalten	nicht mehr verletzen würden.

Um den Richtlinienvergleich als Bericht anzuzeigen

- Wählen Sie den Bericht **Regelvergleich anzeigen**.

Verwandte Themen

- [Unternehmensrichtlinien erstellen und bearbeiten](#) auf Seite 11

Zusätzliche Aufgaben für Arbeitskopien von Unternehmensrichtlinien

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

Arbeitskopien von Unternehmensrichtlinien aktivieren

Mit der Aktivierung der Arbeitskopie werden Änderungen auf die originale Unternehmensrichtlinie übernommen. Zu einer neuen Arbeitskopie wird eine Unternehmensrichtlinie angelegt. Nur originale Unternehmensrichtlinien werden in der Richtlinienprüfung berücksichtigt.

Um eine Arbeitskopie zu aktivieren

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Arbeitskopie aktivieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **OK**.

TIPP: In der Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien > Geänderte Arbeitskopien** werden alle Arbeitskopien angezeigt, deren Bedingung nicht identisch ist mit der Bedingung der originalen Unternehmensrichtlinie.

Arbeitskopien von Unternehmensrichtlinien kopieren

Unternehmensrichtlinien können kopiert werden, um beispielsweise komplexe Richtlinienbedingungen nach zu nutzen. Es können sowohl die Arbeitskopien als auch die aktiven Unternehmensrichtlinien als Kopiervorlage genutzt werden.

Um eine Arbeitskopie zu kopieren

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Richtlinie kopieren**.

5. Erfassen Sie einen Namen für die Kopie und klicken Sie **OK**.
Es wird eine Arbeitskopie mit dem angegebenen Namen angelegt.
6. Um die Stammdaten der Kopie sofort zu bearbeiten, klicken Sie **Ja**.
- ODER -
Um die Stammdaten der Kopie später zu bearbeiten, klicken Sie **Nein**.

Verwandte Themen

- [Unternehmensrichtlinien kopieren](#) auf Seite 25

Bedingungen von Arbeitskopien von Unternehmensrichtlinien anzeigen

Die Datenbankabfrage, über die die Objekte ermittelt werden, welche die Unternehmensrichtlinie verletzen, wird standardmäßig nicht auf dem Stammdatenformular angezeigt.

Um die Datenbankabfrage auf dem Stammdatenformular anzuzeigen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Bedingung anzeigen**.

Um die Datenbankabfrage auf dem Stammdatenformular auszublenden

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Bedingung ausblenden**.

Verwandte Themen

- [Bedingungen von Unternehmensrichtlinien anzeigen](#) auf Seite 26

Ausgewählte Objekte für Arbeitskopien anzeigen

Mit dieser Aufgabe wird eine Liste der Objekte, die durch die Bedingung ermittelt werden, auf dem Stammdatenformular angezeigt.

Um eine Liste der ermittelten Objekte anzuzeigen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Zeige ausgewählte Objekte**.

Auf dem Stammdatenformular wird zusätzliche der Tabreiter **Ergebnis** eingeblendet. Dieser zeigt eine Liste aller Objekte, die durch die Datenbankabfrage ermittelt werden.

Verwandte Themen

- [Ausgewählte Objekte für Unternehmensrichtlinien anzeigen](#) auf Seite 26

Ausnahmegenehmiger für Arbeitskopien pflegen

Über diese Aufgabe können Sie die Ausnahmegenehmiger für die ausgewählte Unternehmensrichtlinie pflegen. Identitäten können der auf dem Stammdatenformular eingetragenen Anwendungsrolle für Ausnahmegenehmiger zugewiesen und aus der Anwendungsrolle entfernt werden.


HINWEIS: Die Änderungen werden für alle Unternehmensrichtlinien wirksam, denen diese Anwendungsrolle zugewiesen ist.

Um Identitäten als Ausnahmegenehmiger zu berechtigen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Ausnahmegenehmiger pflegen**.
4. 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 .
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Allgemeine Stammdaten für Unternehmensrichtlinien](#) auf Seite 12
- [Ausnahmegenehmiger für Richtlinienverletzungen](#) auf Seite 41
- [Ausnahmegenehmiger für Unternehmensrichtlinien pflegen](#) auf Seite 27

Richtlinienverantwortliche für Arbeitskopien pflegen

Über diese Aufgabe können Sie die Richtlinienverantwortlichen für die ausgewählte Unternehmensrichtlinie pflegen. Identitäten können der auf dem Stammdatenformular eingetragenen Anwendungsrolle für Richtlinienverantwortliche zugewiesen und aus der Anwendungsrolle entfernt werden.


HINWEIS: Die Änderungen werden für alle Unternehmensrichtlinien wirksam, denen diese Anwendungsrolle zugewiesen ist.

Um Identitäten als Richtlinienverantwortliche zu berechtigen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Verantwortliche pflegen**.
4. 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 .
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Allgemeine Stammdaten für Unternehmensrichtlinien](#) auf Seite 12
- [Richtlinienverantwortliche für Unternehmensrichtlinien](#) auf Seite 39
- [Richtlinienverantwortliche für Unternehmensrichtlinien pflegen](#) auf Seite 27

Compliance Frameworks an Arbeitskopien von Unternehmensrichtlinien zuweisen

Über diese Aufgabe legen Sie fest, welche Compliance Frameworks für die ausgewählte Unternehmensrichtlinie relevant sind. Compliance Frameworks dienen zur Einstufung von Unternehmensrichtlinien entsprechend regulatorischer Anforderungen.


Um Compliance Frameworks an eine Unternehmensrichtlinie zuzuweisen

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

3. Wählen Sie die Aufgabe **Compliance Frameworks zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Compliance Frameworks zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie das Compliance Framework und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Risikomindernde Maßnahmen an Arbeitskopien zuweisen


Risikomindernde Maßnahmen beschreiben Maßnahmen, die umgesetzt werden sollen, wenn eine Unternehmensrichtlinie verletzt wurde. Nach Umsetzung der Maßnahmen sollte die nächste Richtlinienprüfung keine Richtlinienverletzung ermitteln. Legen Sie fest, welche risikomindernden Maßnahmen für die ausgewählte Unternehmensrichtlinie gelten.

Um risikomindernde Maßnahmen an eine Unternehmensrichtlinie zuzuweisen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Risikomindernde Maßnahmen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die risikomindernden Maßnahmen zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die risikomindernde Maßnahme und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- [Risikomindernde Maßnahmen für Unternehmensrichtlinien](#) auf Seite 60

Überblick über Arbeitskopien anzeigen

Auf dem Überblicksformular erhalten Sie auf einen Blick die wichtigsten Informationen zu einer Arbeitskopie.

Um einen Überblick über eine Arbeitskopie zu erhalten

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Überblick über die Richtlinie**.

Verwandte Themen

- [Überblick über Unternehmensrichtlinien anzeigen](#) auf Seite 29

Zusätzliche Aufgaben für Unternehmensrichtlinien

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

Unternehmensrichtlinien aktivieren und deaktivieren

Damit Richtlinienverletzungen für eine Unternehmensrichtlinie ermittelt werden können, aktivieren Sie die Unternehmensrichtlinie. Um Unternehmensrichtlinien von der Richtlinienprüfung auszuschließen, können Sie die Richtlinie deaktivieren. Dabei entfernt der DBQueue Prozessor alle Informationen über Richtlinienverletzungen für diese Unternehmensrichtlinie aus der Datenbank. Die Arbeitskopie einer Unternehmensrichtlinie ist immer deaktiviert.

Um eine Unternehmensrichtlinie zu aktivieren

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Richtlinie aktivieren**.

Um eine Unternehmensrichtlinie zu deaktivieren

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Richtlinie deaktivieren**.

Arbeitskopien für Unternehmensrichtlinien erstellen

Um eine bestehende Unternehmensrichtlinie zu ändern, benötigen Sie eine Arbeitskopie dieser Unternehmensrichtlinie. Die Arbeitskopie kann aus der aktiven Unternehmensrichtlinie erstellt werden. Die Daten der bestehenden Arbeitskopie werden dabei auf Nachfrage mit den Daten der aktiven Unternehmensrichtlinie überschrieben.

Um eine Arbeitskopie zu erstellen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Arbeitskopie erstellen**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

TIPP: In der Kategorie **Unternehmensrichtlinien > Richtlinien > Arbeitskopien von Richtlinien > Geänderte Arbeitskopien** werden alle Arbeitskopien angezeigt, deren Bedingung nicht identisch ist mit der Bedingung der originalen Unternehmensrichtlinie.

Verwandte Themen

- [Unternehmensrichtlinien erstellen und bearbeiten](#) auf Seite 11
- [Arbeitskopien von Unternehmensrichtlinien aktivieren](#) auf Seite 19

Unternehmensrichtlinien kopieren

Unternehmensrichtlinien können kopiert werden, um beispielsweise komplexe Richtlinienbedingungen nach zu nutzen. Es können sowohl die Arbeitskopien als auch die aktiven Unternehmensrichtlinien als Kopiervorlage genutzt werden.

Um eine Unternehmensrichtlinie zu kopieren

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Richtlinie kopieren**.
5. Erfassen Sie einen Namen für die Kopie und klicken Sie **OK**.
Es wird eine Arbeitskopie mit dem angegebenen Namen angelegt.
6. Um die Stammdaten der Kopie sofort zu bearbeiten, klicken Sie **Ja**.
- ODER -
Um die Stammdaten der Kopie später zu bearbeiten, klicken Sie **Nein**.

Verwandte Themen

- [Arbeitskopien von Unternehmensrichtlinien kopieren](#) auf Seite 19

Bedingungen von Unternehmensrichtlinien anzeigen

Die Datenbankabfrage, über die die Objekte ermittelt werden, die die Unternehmensrichtlinie verletzen, wird standardmäßig nicht auf dem Stammdatenformular angezeigt.

Um die Datenbankabfrage auf dem Stammdatenformular anzuzeigen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Bedingung anzeigen**.

Um die Datenbankabfrage auf dem Stammdatenformular auszublenden

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Bedingung ausblenden**.

Verwandte Themen

- [Bedingungen von Arbeitskopien von Unternehmensrichtlinien anzeigen](#) auf Seite 20

Ausgewählte Objekte für Unternehmensrichtlinien anzeigen

Mit dieser Aufgabe wird eine Liste der Objekte, die durch die Bedingung ermittelt werden, auf dem Stammdatenformular angezeigt.

Um eine Liste der ermittelten Objekte anzuzeigen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Zeige ausgewählte Objekte**.

Auf dem Stammdatenformular wird zusätzlich der Tabreiter **Ergebnis** eingeblendet. Dieser zeigt eine Liste aller Objekte, die durch die Datenbankabfrage ermittelt werden.

Verwandte Themen

- [Ausgewählte Objekte für Arbeitskopien anzeigen](#) auf Seite 20

Ausnahmegenehmiger für Unternehmensrichtlinien pflegen

Über diese Aufgabe können Sie die Ausnahmegenehmiger für die ausgewählte Unternehmensrichtlinie pflegen. Identitäten können der auf dem Stammdatenformular eingetragenen Anwendungsrolle für Ausnahmegenehmiger zugewiesen und aus der Anwendungsrolle entfernt werden.


HINWEIS: Die Änderungen werden für alle Unternehmensrichtlinien wirksam, denen diese Anwendungsrolle zugewiesen ist.

Um Identitäten als Ausnahmegenehmiger zu berechtigen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Ausnahmegenehmiger pflegen**.
4. 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 .
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Allgemeine Stammdaten für Unternehmensrichtlinien](#) auf Seite 12
- [Ausnahmegenehmiger für Richtlinienverletzungen](#) auf Seite 41
- [Ausnahmegenehmiger für Arbeitskopien pflegen](#) auf Seite 21

Richtlinienverantwortliche für Unternehmensrichtlinien pflegen

Über diese Aufgabe können Sie die Richtlinienverantwortlichen für die ausgewählte Unternehmensrichtlinie pflegen. Identitäten können der auf dem Stammdatenformular

eingetragenen Anwendungsrolle für Richtlinienverantwortliche zugewiesen und aus der Anwendungsrolle entfernt werden.


HINWEIS: Die Änderungen werden für alle Unternehmensrichtlinien wirksam, denen diese Anwendungsrolle zugewiesen ist.

Um Identitäten als Richtlinienverantwortliche zu berechtigen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Verantwortliche pflegen**.
4. 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 .
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Allgemeine Stammdaten für Unternehmensrichtlinien](#) auf Seite 12
- [Richtlinienverantwortliche für Unternehmensrichtlinien](#) auf Seite 39
- [Richtlinienverantwortliche für Arbeitskopien pflegen](#) auf Seite 22

Attestierungsvorgänge erstellen

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

Wenn einer Unternehmensrichtlinie eine Attestierungsrichtlinie zugeordnet ist, werden für Richtlinienverletzungen automatisch Attestierungsvorgänge erstellt. Die Attestierung kann bei Bedarf auch manuell gestartet werden. Der Prozess erstellt Attestierungsvorgänge für alle Richtlinienverletzungen der gewählten Unternehmensrichtlinie.

Um die Attestierung von Richtlinienverletzungen manuell zu starten

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Attestierungsvorgänge jetzt erstellen**.

Verwandte Themen

- [Automatische Attestierung von Richtlinienverletzungen](#) auf Seite 56
- [Fehler bei der Attestierung von Richtlinienverletzungen](#) auf Seite 58

- [Attestierung von Richtlinienverletzungen starten](#) auf Seite 57

Überblick über Unternehmensrichtlinien anzeigen

Auf dem Überblicksformular erhalten Sie auf einen Blick die wichtigsten Informationen zu einer Unternehmensrichtlinie.

Um einen Überblick über eine Unternehmensrichtlinie zu erhalten

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Überblick über die Richtlinie**.

Verwandte Themen

- [Überblick über Arbeitskopien anzeigen](#) auf Seite 23

Standard-Unternehmensrichtlinien verwenden

Der One Identity Manager stellt verschiedene Standard-Unternehmensrichtlinien als Arbeitskopien bereit. Damit diese Unternehmensrichtlinien bei der Richtlinienprüfung berücksichtigt werden, aktivieren Sie die Arbeitskopien.

Um eine Standard-Unternehmensrichtlinie zu nutzen

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**.

Für Standard-Unternehmensrichtlinien können folgende Eigenschaften unternehmensspezifisch geändert werden:

- Verantwortliche
- Ausnahmegenehmigung möglich
- Ausnahmegenehmiger
- Hinweise zur Ausnahmegenehmigung
- Attestierer

- Bewertungskriterien
- Attestierungsrichtlinie

TIPP: Wenn Sie weitere Eigenschaften bearbeiten wollen, erstellen Sie eine Kopie der Standard-Unternehmensrichtlinie. An der Kopie können Sie diese Eigenschaften bearbeiten.

Verwandte Themen

- [Risikobewertung für Richtlinienverletzungen](#) auf Seite 15
- [Allgemeine Stammdaten für Unternehmensrichtlinien](#) auf Seite 12
- [Arbeitskopien von Unternehmensrichtlinien kopieren](#) auf Seite 19


Unternehmensrichtlinien löschen

WICHTIG: Wenn Sie eine Unternehmensrichtlinie löschen, werden alle Informationen über die Unternehmensrichtlinie und Richtlinienverletzungen unwiderruflich gelöscht! Die Informationen können zu einem späteren Zeitpunkt nicht wiederhergestellt werden.

Erstellen Sie vor dem Löschen einen Bericht über die Unternehmensrichtlinie und ihre aktuellen Richtlinienverletzungen, wenn Sie die Informationen (beispielsweise zur Revisionsicherheit) aufbewahren wollen.

Eine Unternehmensrichtlinie kann gelöscht werden, wenn keine Richtlinienverletzungen für die Unternehmensrichtlinie vorhanden sind.


Um eine Unternehmensrichtlinie zu löschen:

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die zu löschende Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Richtlinie deaktivieren**.
Vorhandene Richtlinienverletzung werden durch den DBQueue Prozessor entfernt.
4. Nachdem der DBQueue Prozessor die Richtlinienverletzungen für die Unternehmensrichtlinie neu berechnet hat, klicken Sie in den Symbolleisten , um die Unternehmensrichtlinie zu löschen.
Die Unternehmensrichtlinie und die zugehörige Arbeitskopie werden gelöscht.

Richtliniengruppen

Richtliniengruppen nutzen Sie zur funktionalen Zusammenfassung von Unternehmensrichtlinien. Über Richtliniengruppen können Sie die Unternehmensrichtlinien hierarchisch strukturieren.

Um eine Richtliniengruppe zu erstellen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Richtliniengruppen**.
2. Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Richtliniengruppe.
 - **Name der Gruppe:** Bezeichnung der Richtliniengruppe.
 - **Übergeordnete Gruppe:** Übergeordnete Richtliniengruppe in einer Hierarchie. Wählen Sie aus der Auswahlliste eine übergeordnete Richtliniengruppe aus, um Richtliniengruppen hierarchisch zu organisieren
4. Speichern Sie die Änderungen.

Um eine Richtliniengruppe zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Richtliniengruppen**.
2. Wählen Sie in der Ergebnisliste eine Richtliniengruppe. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Bearbeiten Sie die Stammdaten der Richtliniengruppe.
4. Speichern Sie die Änderungen.

Im Bericht **Überblick der Richtlinienverletzungen** erhalten Sie eine Zusammenfassung über alle Richtlinienverletzungen einer Richtliniengruppe.

Compliance Frameworks

Compliance Frameworks dienen zur Einstufung von Attestierungsrichtlinien, Complianceregeln und Unternehmensrichtlinien entsprechend regulatorischer Anforderungen, wie beispielsweise interner Anforderungen oder Anforderungen laut Wirtschaftsprüfung.

Compliance Frameworks können hierarchisch organisiert werden. Ordnen Sie dafür den Compliance Frameworks ein übergeordnetes Framework zu.

Um Compliance Frameworks zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Compliance Frameworks**.
2. Wählen Sie in der Ergebnisliste ein Compliance Framework und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
 - ODER -
 - Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Compliance Frameworks.
4. Speichern Sie die Änderungen.

Für Compliance Frameworks erfassen Sie folgende Eigenschaften.

Tabelle 6: Eigenschaften eines Compliance Frameworks

Eigenschaft	Beschreibung
Compliance Framework	Bezeichnung des Compliance Frameworks.
Übergeordnetes Framework	Übergeordnetes Compliance Framework in der Hierarchie der Compliance Frameworks. Wählen Sie aus der Auswahlliste ein vorhandes Compliance Framework aus, um die Compliance Frameworks hierarchisch zu organisieren.
Verantwortliche	Anwendungsrolle, deren Mitglieder alle Unternehmensrichtlinien bearbeiten dürfen, die diesem Compliance Framework zugeordnet sind.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Compliance Frameworks an Unternehmensrichtlinien zuweisen


Über diese Aufgabe weisen Sie Unternehmensrichtlinien an das ausgewählte Compliance Framework zu.

Um Unternehmensrichtlinien an Compliance Frameworks zuzuweisen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Compliance Frameworks**.
2. Wählen Sie in der Ergebnisliste das Compliance Framework.
3. Wählen Sie die Aufgabe **Unternehmensrichtlinien zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Unternehmensrichtlinien zu.

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

Um eine Zuweisung zu entfernen

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

Überblick über Compliance Frameworks anzeigen

Auf dem Überblicksformular erhalten Sie auf einen Blick die wichtigsten Informationen zu einem Compliance Framework.

Im Bericht **Überblick der Richtlinienverletzungen** erhalten Sie eine Zusammenfassung über alle Richtlinienverletzungen eines Compliance Frameworks.

Um einen Überblick über ein Compliance Framework zu erhalten

1. Wählen Sie die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Compliance Frameworks**.
2. Wählen Sie in der Ergebnisliste das Compliance Framework.
3. Wählen Sie die Aufgabe **Überblick über das Compliance Framework**.

Zeitpläne für die Richtlinienprüfung

Die regelmäßige Überprüfung der Unternehmensrichtlinien wird über Zeitpläne gesteuert. In der One Identity Manager-Standardinstallation wird jeder neuen Unternehmensrichtlinie der Zeitplan **Richtlinienprüfung** zugewiesen. Dieser Zeitplan erzeugt in regelmäßigen Abständen für jede Unternehmensrichtlinie einen Verarbeitungsauftrag für den DBQueue Prozessor. Um den Zyklus der Richtlinienprüfung Ihren Erfordernissen anzupassen, können Sie eigene Zeitpläne einrichten. Stellen Sie sicher, dass diese Zeitpläne den Unternehmensrichtlinien zugewiesen sind.


Um Zeitpläne zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Zeitpläne**.

In der Ergebnisliste werden alle Zeitpläne angezeigt, die für die Tabelle QERPolicy konfiguriert sind.

2. Wählen Sie in der Ergebnisliste einen Zeitplan aus und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.



– ODER –

Klicken Sie in der Ergebnisliste .

3. Bearbeiten Sie die Stammdaten des Zeitplans.
4. Speichern Sie die Änderungen.

Für einen Zeitplan erfassen Sie folgende Eigenschaften.

Tabelle 7: Eigenschaften für einen Zeitplan

Eigenschaft	Bedeutung
Bezeichnung	Bezeichnung des Zeitplanes. Übersetzen Sie den eingegebenen Text über die Schaltfläche  .
Beschreibung	Nähere Beschreibung des Zeitplans. Übersetzen Sie den eingegebenen Text über die Schaltfläche  .
Aktiviert	Gibt an, ob der Zeitplan aktiv ist. HINWEIS: Nur Zeitpläne, die aktiv sind, werden ausgeführt. Aktive Zeitpläne werden automatisiert ausgeführt, wenn der Konfigurationsparameter QBM Schedules aktiviert ist.
Zeitzone	Eindeutige Kennung der Zeitzone, nach dessen Zeitangaben der Zeitplan ausgeführt werden soll. Wählen Sie in der Auswahlliste zwischen Universal Time Code oder einer der Zeitzonen. HINWEIS: Wenn ein neuer Zeitplan angelegt wird, ist die Zeitzone des Clients vorausgewählt, von dem Sie den Manager gestartet haben.
Beginn (Datum)	Tag, an dem der Zeitplan erstmalig ausgeführt werden soll. Falls sich dieser Tag mit dem definierten Intervalltyp widerspricht, ist die erstmalige Ausführung der nächste erreichbare Tag basierend auf dem Startdatum.
Gültigkeitszeitraum	Zeitraum, innerhalb dessen der Zeitplan ausgeführt werden soll. <ul style="list-style-type: none">• Wenn der Zeitplan unbefristet ausgeführt werden soll, wählen Sie die Option Unbegrenzte Laufzeit.• Um einen Gültigkeitszeitraum festzulegen, wählen Sie die Option Begrenzte Laufzeit und erfassen Sie im Eingabefeld Ende (Datum) den Tag, an dem der Zeitplan letztmalig ausgeführt werden soll.
Auftreten	Intervall, in welchem der Auftrag ausgeführt wird. Abhängig vom gewählten Intervall sind weitere Einstellungen erforderlich. <ul style="list-style-type: none">• minütlich: Der Zeitplan soll minütlich ausgeführt werden. Der Startzeitpunkt wird aus der Ausführungsfrequenz und dem Intervalltyp berechnet.• stündlich: Der Zeitplan soll in einem definierten Intervall von Stunden ausgeführt werden, beispielsweise alle zwei Stunden.<ul style="list-style-type: none">• Legen Sie unter Wiederholen alle fest, nach wie vielen Stunden der Zeitplan wiederholt ausgeführt werden soll.

- Der Startzeitpunkt wird aus der Ausführungsfrequenz und dem Intervalltyp berechnet.
- **täglich**: Der Zeitplan soll zu definierten Uhrzeiten in einem definierten Intervall von Tagen ausgeführt werden, beispielsweise jeden zweiten Tag um 6:00 Uhr und um 18:00 Uhr.
 - Legen Sie unter **Startzeit** die Uhrzeiten fest, zu denen der Zeitplan ausgeführt werden soll.
 - Legen Sie unter **Wiederholen alle** fest, nach wie vielen Tagen der Zeitplan wiederholt werden soll.
- **wöchentlich**: Der Zeitplan soll in einem definierten Intervall von Wochen, an einem bestimmten Wochentag, zu definierten Uhrzeiten ausgeführt werden, beispielsweise jede zweite Woche am Montag um 6:00 Uhr und um 18:00 Uhr.
 - Legen Sie unter **Startzeit** die Uhrzeiten fest, zu denen der Zeitplan ausgeführt werden soll.
 - Legen Sie unter **Wiederholen alle** fest, nach wie vielen Wochen der Zeitplan wiederholt ausgeführt werden soll.
 - Legen Sie den genauen Wochentag fest, an dem der Zeitplan ausgeführt werden soll.
- **monatlich**: Der Zeitplan soll in einem definierten Intervall von Monaten, an bestimmten Tagen, zu definierten Uhrzeiten ausgeführt werden, beispielsweise jeden zweiten Monat am 1. Tag und am 15. Tag jeweils um 6:00 Uhr und um 18:00 Uhr.
 - Legen Sie unter **Startzeit** die Uhrzeiten fest, zu denen der Zeitplan ausgeführt werden soll.
 - Legen Sie unter **Wiederholen alle** fest, nach wie vielen Monaten der Zeitplan wiederholt werden soll.
 - Legen Sie die Tage des Monats fest (1.-31. Tag eines Monats).

HINWEIS: Wenn es beim Intervalltyp **monatlich** mit dem Subintervall **29, 30** oder **31** den Ausführungstag im aktuellen Monat nicht gibt, so wird der letzte Tag des Monats verwendet.

Beispiel:

Ein Zeitplan der monatlich am 31. Tag ausgeführt werden soll, wird im April am 30. ausgeführt. Im Februar wird der Zeitplan am 28. (am 29. in Schaltjahren) ausgeführt.

Eigenschaft

Bedeutung

- **jährlich:** Der Zeitplan soll in einem definierten Intervall von Jahren, an bestimmten Tagen, zu definierten Uhrzeiten ausgeführt werden, beispielsweise jedes Jahr am 1.Tag, am 100. Tag und am 200.Tag jeweils um 6:00 Uhr und um 18:00 Uhr.
 - Legen Sie unter **Startzeit** die Uhrzeiten fest, zu denen der Zeitplan ausgeführt werden soll.
 - Legen Sie unter **Wiederholen alle** fest, nach wie vielen Jahren der Zeitplan wiederholt werden soll.
 - Legen Sie die Tage des Jahres fest (1. bis 366.Tag eines Jahres).

HINWEIS: Wenn der 366. Tag des Jahres gewählt wird, wird der Zeitplan nur in Schaltjahren ausgeführt.
- **Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag:** Der Zeitplan soll an einem bestimmten Wochentag, in definierten Monaten, zu definierten Uhrzeiten ausgeführt werden, beispielsweise am zweiten Samstag im Januar und im Juni um 10:00 Uhr.
 - Legen Sie unter **Startzeit** die Uhrzeiten fest, zu denen der Zeitplan ausgeführt werden soll.
 - Legen Sie unter **Wiederholen alle** fest, am wievielten Wochentag eines Monats der Zeitplan ausgeführt werden soll. Zulässig sind die Werte **1 bis 4, -1** (letzter entsprechender Wochentag) und **-2** (vorletzter entsprechender Wochentag).
 - Legen Sie den Monat fest, in welchem der Zeitplan ausgeführt werden soll. Zulässig sind die Werte **1 bis 12**. Ist der Wert leer, wird der Zeitplan in jedem Monat ausgeführt.

Startzeit

Feste Startzeit. Geben Sie die Uhrzeit in der Ortszeit der ausgewählten Zeitzone an. Bei einer Liste von Startzeiten wird der Zeitplan zu jeder dieser Zeiten gestartet.

Wiederholen alle

Ausführungsfrequenz, mit welcher der zeitgesteuerte Auftrag innerhalb des gewählten Zeitintervalls ausgeführt werden soll.

Letzter geplanter Lauf/Nächster geplanter Lauf

Ausführungszeitpunkte, die durch den DBQueue Prozessor berechnet wurden. Die Ausführungszeitpunkte werden während der Ausführung eines Zeitplans neu ermittelt. Der Zeitpunkt der nächsten Ausführung wird anhand des festgelegten Intervalls, der Ausführungsfrequenz und der Startzeit berechnet.

HINWEIS: Der One Identity Manager zeigt die Ausführungszeitpunkte in der Ortszeit der ausgewählten Zeitzone an. Sommerzeitumstellungen werden bei der Berechnung berücksichtigt.

Unternehmensrichtlinien an Zeitpläne zuweisen

Über diese Aufgabe weisen Sie dem ausgewählten Zeitplan die Unternehmensrichtlinien zu, die mit diesem Zeitplan ausgeführt werden sollen. Über das Zuordnungsformular können Sie den ausgewählten Zeitplan an beliebige Unternehmensrichtlinien zuweisen.

Standardmäßig wird einer Unternehmensrichtlinien der Zeitplan **Richtlinienprüfung** zugewiesen.

HINWEIS: Zuordnungen können nicht entfernt werden. Die Zuordnung eines Zeitplans ist für Unternehmensrichtlinien eine Pflichteingabe.

Um einen Zeitplan an Unternehmensrichtlinien zuzuweisen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Zeitpläne**.
2. Wählen Sie in der Ergebnisliste den Zeitplan.
3. Wählen Sie die Aufgabe **Unternehmensrichtlinien zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Unternehmensrichtlinien zu.
5. Speichern Sie die Änderungen.

Um eine Zuordnung zu ändern

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Zeitpläne**.
2. Wählen Sie in der Ergebnisliste den Zeitplan.
3. Wählen Sie die Aufgabe **Unternehmensrichtlinien zuweisen**.
4. Wählen Sie im Kontextmenü des Zuordnungsformulars **Zeige bereits anderen Objekten zugewiesene Objekte**.

Es werden die Unternehmensrichtlinien eingeblendet, die bereits anderen Zeitplänen zugewiesen sind.

5. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf eine dieser Unternehmensrichtlinien.
Dieser Unternehmensrichtlinie wird der aktuell ausgewählte Zeitplan zugeordnet.
6. Speichern Sie die Änderungen.
7. Damit die Änderung wirksam wird, aktivieren Sie die Arbeitskopie.

Verwandte Themen

- [Arbeitskopien von Unternehmensrichtlinien aktivieren](#) auf Seite 19
- [Erweiterte Angaben für Unternehmensrichtlinien](#) auf Seite 17

Zeitpläne sofort ausführen

Um einen Zeitplan sofort zu starten

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Zeitpläne**.
2. Wählen Sie in der Ergebnisliste den Zeitplan.
3. Wählen Sie die Aufgabe **Sofort ausführen**.

Es erscheint eine Meldung, die bestätigt, dass der Zeitplan gestartet wurde.

Überblick über Zeitpläne anzeigen

Auf dem Überblicksformular erhalten Sie auf einen Blick die wichtigsten Informationen zu einem Zeitplan.

Um einen Überblick über einen Zeitplan zu erhalten

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Zeitpläne**.
2. Wählen Sie in der Ergebnisliste den Zeitplan.
3. Wählen Sie die Aufgabe **Überblick zum Zeitplan**.

Attestierer für Unternehmensrichtlinien

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

An Unternehmensrichtlinien können Identitäten zugewiesen werden, die als verantwortliche Attestierer für Attestierungsvorgänge herangezogen werden können. Dazu ordnen Sie den Unternehmensrichtlinien eine Anwendungsrolle für Attestierer zu. Dieser Anwendungsrolle weisen Sie die Identitäten zu, die berechtigt sind, die Gültigkeit dieser Unternehmensrichtlinie zu attestieren. Ausführliche Informationen zur Attestierung finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*.

Im One Identity Manager ist eine Standardanwendungsrolle für Attestierer vorhanden. Bei Bedarf können Sie weitere Anwendungsrollen erstellen. Ausführliche Informationen zu

Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Tabelle 8: Standardanwendungsrolle für Attestierer


Benutzer	Aufgaben
Attestierer für Unternehmensrichtlinien	<p>Die Attestierer müssen der Anwendungsrolle Identity & Access Governance Unternehmensrichtlinien Attestierer zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Attestieren im Web Portal die Unternehmensrichtlinien und Ausnahmegenehmigungen, für die sie verantwortlich sind.• Können die Stammdaten der Unternehmensrichtlinien sehen, aber nicht bearbeiten. <p>HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.</p>

Um Identitäten in die Standardanwendungsrolle für Attestierer aufzunehmen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Attestierer**.
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.

Richtlinienverantwortliche für Unternehmensrichtlinien

An Unternehmensrichtlinien können Identitäten zugewiesen werden, die inhaltlich für die Unternehmensrichtlinien verantwortlich sind. Dazu ordnen Sie in den allgemeinen Stammdaten einer Unternehmensrichtlinien eine Anwendungsrolle für Richtlinienverantwortliche zu.

Im One Identity Manager ist eine Standardanwendungsrolle für Richtlinienverantwortliche vorhanden. Bei Bedarf können Sie weitere Anwendungsrollen erstellen. Ausführliche

Informationen zu Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Tabelle 9: Standardanwendungsrolle für Regelverantwortliche


Benutzer	Aufgaben
Richtlinienverantwortliche	<p>Die Richtlinienverantwortlichen müssen der Anwendungsrolle Identity & Access Governance Unternehmensrichtlinien Richtlinienverantwortliche oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Sind inhaltlich verantwortlich für Unternehmensrichtlinien.• Bearbeiten die Arbeitskopien der Unternehmensrichtlinien.• Aktivieren und deaktivieren Unternehmensrichtlinien.• Können bei Bedarf die Berechnung der Richtlinien starten und Richtlinienverletzungen einsehen.• Weisen risikomindernde Maßnahmen zu.

Um Identitäten in die Standardanwendungsrolle für Richtlinienverantwortliche aufzunehmen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Richtlinienverantwortliche**.
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.

Verwandte Themen

- [Richtlinienverantwortliche für Arbeitskopien pflegen](#) auf Seite 22
- [Richtlinienverantwortliche für Unternehmensrichtlinien pflegen](#) auf Seite 27

Ausnahmegenehmiger für Richtlinienverletzungen

An Unternehmensrichtlinien können Identitäten zugewiesen werden, die Ausnahmegenehmigungen für Richtlinienverletzungen erteilen dürfen. Dazu ordnen Sie in den allgemeinen Stammdaten einer Unternehmensrichtlinie eine Anwendungsrolle für Ausnahmegenehmiger zu.

Im One Identity Manager ist eine Standardanwendungsrolle für Ausnahmegenehmiger vorhanden. Bei Bedarf können Sie weitere Anwendungsrollen erstellen. Ausführliche Informationen zu Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Tabelle 10: Standardanwendungsrolle für Ausnahmegenehmiger


Benutzer	Aufgaben
Ausnahmegenehmiger	<p>Die Ausnahmegenehmiger müssen der Anwendungsrolle Identity & Access Governance Unternehmensrichtlinien Ausnahmegenehmiger oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Bearbeiten die Richtlinienverletzungen.• Können Ausnahmegenehmigungen erteilen oder entziehen.

Um Identitäten in die Standardanwendungsrolle für Ausnahmegenehmiger aufzunehmen

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.

Verwandte Themen


- [Erteilen von Ausnahmegenehmigungen](#) auf Seite 51
- [Ausnahmegenehmiger für Arbeitskopien pflegen](#) auf Seite 21

- [Ausnahmegenehmiger für Unternehmensrichtlinien pflegen](#) auf Seite 27

Standardbegründungen für Richtlinienverletzungen

Bei Ausnahmegenehmigungen können im Web Portal Begründungen angegeben werden, welche die einzelnen Entscheidungen erläutern. Diese Begründungen können als Freitext formuliert werden. Darüber hinaus gibt es die Möglichkeit Begründungstexte vorzuformulieren. Aus diesen Standardbegründungen können die Ausnahmegenehmiger im Web Portal einen geeigneten Text auswählen und an der Richtlinienverletzung hinterlegen.

Um Standardbegründungen zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten > Standardbegründungen**.
2. Wählen Sie in der Ergebnisliste eine Standardbegründung und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
- ODER -
Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Standardbegründung.
4. Speichern Sie die Änderungen.

Für eine Standardbegründung erfassen Sie folgende Eigenschaften.

Tabelle 11: Allgemeine Stammdaten einer Standardbegründung

Eigenschaft	Beschreibung
Standardbegründung	Begründungstext, so wie er im Web Portal angezeigt werden soll.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatische Entscheidung	Angabe, ob der Begründungstext nur bei automatischen Entscheidungen durch den One Identity Manager an der Richtlinienverletzung eingetragen werden soll. Diese Standardbegründung kann bei Ausnahmegenehmigungen im Web Portal nicht ausgewählt werden. Damit die Standardbegründung im Web Portal ausgewählt werden kann, deaktivieren Sie die Option.
Zusätzlicher Text erforderlich	Angabe, ob bei der Ausnahmegenehmigung eine zusätzliche Begründung als Freitext erfasst werden soll.
Nutzungstyp	Nutzungstyp der Standardbegründung. Um Standard-

Eigenschaft	Beschreibung
	begründungen im Web Portal filtern zu können, ordnen Sie einen oder mehrere Nutzungstypen zu.

Verwandte Themen

- [Vordefinierte Standardbegründungen für Richtlinienverletzungen](#) auf Seite 43

Vordefinierte Standardbegründungen für Richtlinienverletzungen

Der One Identity Manager stellt vordefinierte Standardbegründungen bereit. Diese Standardbegründungen werden bei automatischen Entscheidungen durch den One Identity Manager an der Richtlinienverletzung eingetragen. Über den Nutzungstyp können Sie festlegen, welche Standardbegründungen im Web Portal ausgewählt werden können.

Um den Nutzungstyp zu ändern

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten > Standardbegründungen > Vordefiniert**.
2. Wählen Sie die Standardbegründung, deren Nutzungstyp Sie ändern möchten.
3. Führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
4. Aktivieren Sie im Auswahlfeld **Nutzungstyp** alle Funktionen, für welche die Standardbegründung im Web Portal angezeigt werden soll.
Deaktivieren Sie alle Funktionen, für welche die Standardbegründung nicht angezeigt werden soll.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Standardbegründungen für Richtlinienverletzungen](#) auf Seite 42

Mailvorlagen für Benachrichtigungen über Unternehmensrichtlinien

Der One Identity Manager stellt standardmäßig Mailvorlagen bereit. Diese Mailvorlagen werden in den Sprachen Deutsch und Englisch bereitgestellt. Wenn Sie den Mailtext in anderen Sprachen benötigen, können Sie Maildefinitionen für diese Sprachen zu den Standard-Mailvorlagen hinzufügen.

Um Standard-Mailvorlagen zu bearbeiten

- Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Mailvorlagen > Vordefiniert**.

Verwandte Themen

- [Maildefinitionen für Unternehmensrichtlinien erstellen und bearbeiten](#) auf Seite 44
- [Basisobjekte für Mailvorlagen für Unternehmensrichtlinien](#) auf Seite 45
- [Mailvorlagen für Unternehmensrichtlinien bearbeiten](#) auf Seite 45
- [Verwenden von Hyperlinks zum Web Portal](#) auf Seite 47
- [Standardfunktionen für die Erstellung von Hyperlinks](#) auf Seite 48

Maildefinitionen für Unternehmensrichtlinien erstellen und bearbeiten

Ausführliche Informationen zum Erstellen und Bearbeiten von Mailvorlagen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.

In einer Mailvorlage können die Mailtexte in den verschiedenen Sprachen definiert werden. Somit wird bei Generierung einer E-Mail-Benachrichtigung die Sprache des Empfängers berücksichtigt.

HINWEIS: Wenn der Konfigurationsparameter **Common | MailNotification | DefaultCulture** aktiviert ist, wird beim Öffnen einer Mailvorlage die Maildefinition in der Standardsprache für E-Mail-Benachrichtigungen geladen und angezeigt.

Um eine neue Maildefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Mailvorlagen**.

In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für Richtlinienprüfungen genutzt werden können.

2. Wählen Sie in der Ergebnisliste eine Mailvorlage und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Wählen Sie in der Auswahlliste **Sprache** die Sprache, für welche die Maildefinition gelten soll.

Angezeigt werden alle Sprachen, die aktiviert sind. Um weitere Sprachen zu verwenden, aktivieren Sie im Designer die entsprechenden Länder. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

4. Erfassen Sie im Eingabefeld **Betreff** die Betreffzeile.

5. Bearbeiten Sie in der Ansicht **Maildefinition** den Mailbody mit Hilfe des Mailtexteditors.
6. Speichern Sie die Änderungen.

Um eine vorhandene Maildefinition zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Mailvorlagen**.

In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für Richtlinienprüfungen genutzt werden können.

1. Wählen Sie in der Ergebnisliste eine Mailvorlage und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
2. In der Auswahlliste **Maildefinition** wählen Sie die Sprache für die Maildefinition.
3. Bearbeiten Sie die Betreffzeile und den Mailbody.
4. Speichern Sie die Änderungen.

Basisobjekte für Mailvorlagen für Unternehmensrichtlinien

HINWEIS: In Mailvorlagen für Unternehmensrichtlinien verwenden Sie die Basisobjekte `QERPolicy` oder `QERPolicyHasObject`.

In der Betreffzeile und im Mailbody einer Maildefinition können Sie alle Eigenschaften des unter **Basisobjekt** eingetragenen Objektes verwenden. Zusätzlich können Sie die Eigenschaften der Objekte verwenden, die per Fremdschlüsselbeziehung referenziert werden.

Zum Zugriff auf die Eigenschaften nutzen Sie die `$`-Notation. Ausführliche Informationen zur Verwendung `$`-Notation finden Sie im *One Identity Manager Konfigurationshandbuch*.

Mailvorlagen für Unternehmensrichtlinien bearbeiten

Ausführliche Informationen zum Erstellen und Bearbeiten von Mailvorlagen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.

Eine Mailvorlage besteht aus allgemeinen Stammdaten wie beispielsweise Zielformat, Wichtigkeit oder Vertraulichkeit der E-Mail Benachrichtigung sowie einer oder mehreren Maildefinitionen. Über die Maildefinitionen werden die Mailtexte in den verschiedenen Sprachen definiert. Somit wird bei Generierung einer E-Mail-Benachrichtigung die Sprache des Empfängers berücksichtigt.

Um Mailvorlagen zu erstellen und zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Mailvorlagen**.

In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für Richtlinienprüfungen genutzt werden können.

2. Wählen Sie in der Ergebnisliste eine Mailvorlage und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

- ODER -

Klicken Sie in der Ergebnisliste .

Der Mailvorlageneditor wird geöffnet.

3. Bearbeiten Sie die Mailvorlage.
4. Speichern Sie die Änderungen.

Um eine Mailvorlage zu kopieren

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Mailvorlagen**.

In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für Richtlinienprüfungen genutzt werden können.

2. Wählen Sie in der Ergebnisliste die Mailvorlage, die Sie kopieren möchten, und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Wählen Sie die Aufgabe **Mailvorlage kopieren**.
4. Erfassen Sie im Eingabefeld **Name der Kopie** den Namen der neuen Mailvorlage.
5. Klicken Sie **OK**.

Um die Vorschau einer Mailvorlage anzuzeigen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Mailvorlagen**.


In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für Richtlinienprüfungen genutzt werden können.

2. Wählen Sie in der Ergebnisliste die Mailvorlage und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Wählen Sie die Aufgabe **Vorschau**.
4. Wählen Sie das Basisobjekt.
5. Klicken Sie **OK**.

Um eine Mailvorlage zu löschen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Basisdaten zur Konfiguration > Mailvorlagen**.

In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für Richtlinienprüfungen genutzt werden können.

2. Wählen Sie in der Ergebnisliste die Mailvorlage.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Verwenden von Hyperlinks zum Web Portal

In den Mailbody einer Maildefinition können Sie Hyperlinks zum Web Portal einfügen. Klickt der Empfänger in der E-Mail Benachrichtigung auf den Hyperlink, wird er auf eine Seite im Web Portal geleitet und kann dort weitere Aktionen ausführen. In der Standardauslieferung wird dieses Verfahren bei Richtlinienprüfungen eingesetzt.

Voraussetzung für die Nutzung dieses Verfahrens

- Der Konfigurationsparameter **QER | WebPortal | BaseURL** ist aktiviert und enthält die URL zum API Server. Den Konfigurationsparameter bearbeiten Sie im Designer.

`http://<Servername>/<Anwendung>`

mit:

<Servername> = Name des Servers

<Anwendung> = Pfad zum API Server Installationsverzeichnis

Um einen Hyperlink zum Web Portal im Mailbody einzufügen

1. Klicken Sie im Mailbody der Maildefinition an die Stelle, an der Sie einen Hyperlink einfügen möchten.
2. Öffnen Sie das Kontextmenü **Hyperlink** und erfassen Sie folgende Informationen.
 - **Text anzeigen:** Erfassen Sie den Anzeigetext des Hyperlinks.
 - **Link zu:** Wählen Sie die Option **Datei oder Webseite**.
 - **Adresse:** Erfassen Sie die Adresse der Seite im Web Portal, die geöffnet werden soll.

HINWEIS: Der One Identity Manager stellt einige Standardfunktionen zur Verfügung, welche Sie für die Erstellung von Hyperlinks zum Web Portal verwenden können.

3. Um die Eingaben zu übernehmen, klicken Sie **OK**.

Standardfunktionen für die Erstellung von Hyperlinks

Zur Erstellung von Hyperlinks werden Ihnen einige Standardfunktionen zur Seite gestellt. Die Funktionen können Sie direkt beim Einfügen eines Hyperlinks im Mailbody einer Maildefinition oder in Prozessen verwenden.

Direkte Eingabe einer Funktion

Eine Funktion wird beim Einfügen eines Hyperlinks über das Kontextmenü **Hyperlink** im Eingabefeld **Adresse** referenziert.

Syntax

```
$Script(<Funktion>)$
```

Beispiel:

```
$Script(VI_BuildQERPolicyLink_Show)$
```

Standardfunktionen für die Richtlinienprüfung

Das Skript `VI_BuildComplianceLinks` enthält eine Sammlung von Standardfunktionen, um Hyperlinks für die Ausnahmegenehmigung von Richtlinienverletzungen zusammenzusetzen.

Tabelle 12: Funktionen des Skriptes `VI_BuildComplianceLinks`

Funktion	Verwendung
<code>VI_BuildQERPolicyLink_Show</code>	Öffnet die Seite zur Ausnahmegenehmigung im Web Portal.

Überprüfen der Unternehmensrichtlinien

Zur Überprüfung einer Unternehmensrichtlinie werden Verarbeitungsaufträge für den DBQueue Prozessor erzeugt. Der DBQueue Prozessor ermittelt für jede Unternehmensrichtlinie, welche Objekte die Unternehmensrichtlinie verletzen. Die für die Unternehmensrichtlinie festgelegten Ausnahmegenehmiger können die Richtlinienverletzungen überprüfen und gegebenenfalls Ausnahmegenehmigungen erteilen.

Detaillierte Informationen zum Thema

- [Berechnen von Richtlinienverletzungen](#) auf Seite 49
- [Berichte über Richtlinienverletzungen](#) auf Seite 51
- [Erteilen von Ausnahmegenehmigungen](#) auf Seite 51
- [Benachrichtigungen über Richtlinienverletzungen](#) auf Seite 52
- [Entscheidungsstatus von Richtlinienverletzungen anzeigen](#) auf Seite 55

Berechnen von Richtlinienverletzungen

Um aktuelle Richtlinienverletzungen in der One Identity Manager Datenbank zu ermitteln, kann die Richtlinienprüfung über verschiedene Wege gestartet werden.

- Zeitgesteuerte Richtlinienprüfung
- Ad-hoc-Richtlinienprüfung

Darüber hinaus wird die Überprüfung einer Unternehmensrichtlinien durch verschiedene Ereignisse ausgelöst.

- Die Unternehmensrichtlinie wird aktiviert.
- Die Arbeitskopie wird aktiviert.
- Die Unternehmensrichtlinie wird deaktiviert.

Bei der Richtlinienprüfung werden alle Objekte ermittelt, welche die in der Unternehmensrichtlinie definierte Bedingung erfüllen. Es werden nur die aktivierten Unternehmensrichtlinien berücksichtigt.

Verwandte Themen

- [Zeitgesteuerte Richtlinienprüfung](#) auf Seite 50
- [Ad-hoc-Richtlinienprüfung](#) auf Seite 50

Zeitgesteuerte Richtlinienprüfung

Für die komplette Überprüfung aller Unternehmensrichtlinien ist in der One Identity Manager-Standardinstallation der Zeitplan **Richtlinienprüfung** enthalten. Dieser Zeitplan erzeugt in regelmäßigen Abständen Verarbeitungsaufträge für den DBQueue Prozessor.

Voraussetzungen

- Die Unternehmensrichtlinie ist aktiviert.
- Der an der Unternehmensrichtlinie hinterlegte Zeitplan ist aktiviert.

Detaillierte Informationen zum Thema

- [Zeitpläne für die Richtlinienprüfung](#) auf Seite 33
- [Unternehmensrichtlinien aktivieren und deaktivieren](#) auf Seite 24

Ad-hoc-Richtlinienprüfung

An einer aktivierten Unternehmensrichtlinie stehen verschiedene Aufgaben zur sofortigen Richtlinienprüfung zur Verfügung.

Um eine ausgewählte Unternehmensrichtlinie sofort zu überprüfen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Richtlinie neu berechnen**.

Um alle Unternehmensrichtlinien sofort zu überprüfen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.

3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Alles neu berechnen**.

Berichte über Richtlinienverletzungen

One Identity Manager stellt verschiedene Berichte zur Verfügung, in denen Informationen über das ausgewählte Basisobjekt und seine Beziehungen zu anderen Objekten der One Identity Manager-Datenbank aufbereitet sind. Für alle aktiven Unternehmensrichtlinien, Richtliniengruppen und Compliance Frameworks können folgende Berichte erstellt werden.

Tabelle 13: Berichte über Richtlinienverletzungen

Bericht	Beschreibung
Überblick der Richtlinienverletzungen (einer Unternehmensrichtlinie)	Der Bericht stellt alle Richtlinienverletzungen für die ausgewählte Unternehmensrichtlinie zusammen. Es werden alle Objekte aufgelistet, die die Unternehmensrichtlinie verletzen. Die Ergebnisliste ist gruppiert nach <ul style="list-style-type: none"> • Richtlinienverletzungen, über die noch entschieden werden muss, • Richtlinienverletzungen ohne Ausnahmegenehmigung, • Richtlinienverletzungen mit Ausnahmegenehmigung.
Überblick der Richtlinienverletzungen (einer Richtliniengruppe)	Der Bericht stellt alle Richtlinienverletzungen für die ausgewählte Richtliniengruppe zusammen. Es werden alle verletzten Unternehmensrichtlinien aufgelistet. Dazu wird die Anzahl der genehmigten, abgelehnten und nicht bearbeiteten Richtlinienverletzungen angegeben.
Überblick der Richtlinienverletzungen (eines Compliance Frameworks)	Der Bericht stellt alle Richtlinienverletzungen für das ausgewählte Compliance Framework zusammen. Es werden alle verletzten Unternehmensrichtlinien aufgelistet. Dazu wird die Anzahl der genehmigten, abgelehnten und nicht bearbeiteten Richtlinienverletzungen angegeben.

Erteilen von Ausnahmegenehmigungen

Mitunter können Unternehmensrichtlinien nicht in jedem Einzelfall eingehalten werden. Richtlinienverletzungen können zeitweilig akzeptiert sein, wenn durch geeignete Maßnahmen sicher gestellt ist, dass diese Richtlinienverletzungen regelmäßig überprüft werden. Für diese Zwecke ist es möglich Ausnahmegenehmigungen für einzelne Richtlinienverletzungen zu erteilen.

Um Ausnahmegenehmigungen zu erteilen, nutzen Sie das Web Portal. Ausführliche Informationen finden Sie im *One Identity Manager Web Portal Anwenderhandbuch*.

Ausnahmegenehmigungen werden an den Richtlinienverletzungen hinterlegt. Auf dem Überblicksformular einer Unternehmensrichtlinie erhalten Sie einen Überblick über alle unbearbeiteten (neuen) Richtlinienverletzungen sowie die erteilten und abgelehnten Ausnahmegenehmigungen.

Voraussetzungen

- An der Unternehmensrichtlinie ist die Option **Ausnahmegenehmigung möglich** aktiviert.
- Der Unternehmensrichtlinie ist eine Anwendungsrolle für Ausnahmegenehmiger zugeordnet.
- Dieser Anwendungsrolle sind Identitäten zugewiesen.

HINWEIS: Wenn die Option **Ausnahmegenehmigung möglich** nachträglich deaktivieren wird, werden unbearbeitete Richtlinienverletzungen für diese Unternehmensrichtlinie automatisch abgelehnt. Bereits erteilte Ausnahmegenehmigungen werden entzogen.

Detaillierte Informationen zum Thema

- [Allgemeine Stammdaten für Unternehmensrichtlinien](#) auf Seite 12
- [Überblick über Unternehmensrichtlinien anzeigen](#) auf Seite 29

Benachrichtigungen über Richtlinienverletzungen

Im Anschluss an die Richtlinienprüfung können E-Mail-Benachrichtigungen über neue Richtlinienverletzungen an die Ausnahmegenehmiger und Richtlinienverantwortlichen gesendet werden. Die Benachrichtigungsverfahren nutzen Mailvorlagen zur Erzeugung der Benachrichtigungen. In einer Mailvorlage sind die Mailtexte in verschiedenen Sprachen definiert. Somit wird bei Generierung einer E-Mail-Benachrichtigung die Sprache des Empfängers berücksichtigt. In der Standardinstallation sind bereits Mailvorlagen enthalten, die Sie zur Konfiguration der Benachrichtigungsverfahren verwenden können.

Benachrichtigungen werden standardmäßig nicht an die zentrale Entscheidergruppe versendet. Fallback-Entscheider werden nur benachrichtigt, wenn für einen Entscheidungsschritt nicht genügend Entscheider ermittelt werden können.

Um E-Mail-Benachrichtigungen zu nutzen

1. Stellen Sie sicher, dass das E-Mail-Benachrichtigungssystem im One Identity Manager konfiguriert ist. Ausführliche Informationen finden Sie im

One Identity Manager Installationshandbuch.

2. Aktivieren Sie im Designer den Konfigurationsparameter **QER | Policy | EmailNotification**.
3. Aktivieren Sie im Designer den Konfigurationsparameter **QER | Policy | EmailNotification | DefaultSenderAddress** und erfassen Sie die Absenderadresse, mit der die E-Mail Benachrichtigungen verschickt werden.
4. Stellen Sie sicher, dass alle Identitäten eine Standard-E-Mail-Adresse besitzen. An diese E-Mail Adresse werden die Benachrichtigungen versendet. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.
5. Stellen Sie sicher, dass für alle Identitäten eine Sprache ermittelt werden kann. Nur so erhalten die Identitäten die E-Mail Benachrichtigungen in ihrer Sprache. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.
6. Konfigurieren Sie die Benachrichtigungsverfahren.

Verwandte Themen

- [Mailvorlagen für Unternehmensrichtlinien bearbeiten](#) auf Seite 45
- [Aufforderung zur Ausnahmegenehmigung](#) auf Seite 53
- [Benachrichtigung über Richtlinienverletzungen ohne Ausnahmegenehmigung](#) auf Seite 54

Aufforderung zur Ausnahmegenehmigung

Wenn bei der Richtlinienprüfung neue Richtlinienverletzungen ermittelt werden, werden die Ausnahmegenehmiger benachrichtigt und zur Entscheidung aufgefordert.

Voraussetzungen

- Ausnahmegenehmigungen für Richtlinienverletzungen sind zulässig.
- Der Unternehmensrichtlinie ist eine Anwendungsrolle **Ausnahmegenehmiger** zugeordnet.
- Dieser Anwendungsrolle sind Identitäten zugewiesen.

Um Aufforderungen zur Ausnahmegenehmigung zu versenden

- Erfassen Sie an der Unternehmensrichtlinie die folgenden Daten.
 - **Ausnahmegenehmigung möglich:** aktiviert
 - **Mailvorlage neue Verletzung:** Richtlinien - Neue Ausnahmegenehmigung erforderlich

TIPP: Um eine andere als die Standardmailvorlage für diese Benachrichtigungen zu nutzen, erstellen Sie eine Mailvorlage mit dem Basisobjekt QERPolicy.

Verwandte Themen

- [Unternehmensrichtlinien erstellen und bearbeiten](#) auf Seite 11
- [Allgemeine Stammdaten für Unternehmensrichtlinien](#) auf Seite 12
- [Mailvorlagen für Unternehmensrichtlinien bearbeiten](#) auf Seite 45

Benachrichtigung über Richtlinienverletzungen ohne Ausnahmegenehmigung

Wenn bei der Überprüfung der Unternehmensrichtlinien neue Richtlinienverletzungen ermittelt werden, für die keine Ausnahmegenehmigung erteilt werden kann, werden die Richtlinienverantwortlichen benachrichtigt.

Voraussetzungen

- Ausnahmegenehmigungen für Richtlinienverletzungen sind nicht zulässig.
- Der Unternehmensrichtlinie ist eine Anwendungsrolle für **Verantwortliche** zugeordnet.
- Dieser Anwendungsrolle sind Identitäten zugewiesen.

Um Richtlinienverantwortliche über Richtlinienverletzungen zu informieren

- Erfassen Sie an der Unternehmensrichtlinie die folgenden Daten.
 - **Ausnahmegenehmigung möglich:** deaktiviert
 - **Mailvorlage neue Verletzung:** Richtlinien - Unzulässige Verletzung aufgetreten

TIPP: Um eine andere als die Standardmailvorlage für diese Benachrichtigungen zu nutzen, erstellen Sie eine Mailvorlage mit dem Basisobjekt QERPolicy.

Verwandte Themen

- [Unternehmensrichtlinien erstellen und bearbeiten](#) auf Seite 11
- [Allgemeine Stammdaten für Unternehmensrichtlinien](#) auf Seite 12
- [Mailvorlagen für Unternehmensrichtlinien bearbeiten](#) auf Seite 45

Entscheidungsstatus von Richtlinienverletzungen anzeigen

Richtlinienverletzungen bearbeiten Sie mit dem Web Portal. Ausführliche Informationen finden Sie im *One Identity Manager Web Portal Anwenderhandbuch*.

Sie können sich im Manager einen Überblick über den Entscheidungsstatus der einzelnen Richtlinienverletzungen verschaffen. Öffnen Sie dafür das Überblicksformular der aktivierten Unternehmensrichtlinie, deren Richtlinienverletzungen Sie betrachten wollen. Hier werden Formularelemente für neue, genehmigte und abgelehnte Richtlinienverletzungen angezeigt.

Um die Details einer Richtlinienverletzung anzuzeigen

1. Wählen Sie im Manager die Kategorie **Unternehmensrichtlinien > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Überblick über die Richtlinie**.
4. Wählen Sie das Formularelement für die Richtlinienverletzung und blenden Sie die Listeneinträge ein. Zur Auswahl stehen:

- **Richtlinienverletzungen: Neu:** Es werden alle Richtlinienverletzungen angezeigt, für die noch keine Entscheidung getroffen wurde.
- **Richtlinienverletzungen: Ausnahme genehmigt:** Es werden alle Richtlinienverletzungen angezeigt, für die eine Ausnahmegenehmigung erfolgt ist.
- **Richtlinienverletzungen: Ausnahme abgelehnt:** Es werden alle Richtlinienverletzungen angezeigt, für die keine Ausnahmegenehmigung erfolgt ist.

5. Klicken Sie auf die Richtlinienverletzung, deren Details Sie ansehen wollen.

Das Stammdatenformular der Richtlinienverletzung wird geöffnet. Sie erhalten einen Überblick über das Objekt, das die Richtlinienverletzung verursacht, den Entscheidungsstatus und den verantwortlichen Ausnahmegenehmiger.

Verwandte Themen

- [Überblick über Unternehmensrichtlinien anzeigen](#) auf Seite 29

Automatische Attestierung von Richtlinienverletzungen

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

Für Richtlinienverletzungen kann eine automatische Rezertifizierung der betroffenen Berechtigungen angeboten werden. Infolge der Rezertifizierung können Berechtigungen, die nicht mehr genutzt werden sollen, automatisch deaktiviert oder entfernt werden. Diese Funktionalität wird standardmäßig im Rahmen des Behavior Driven Governance genutzt. Sie können diese Funktionalität jedoch auch für eigene Unternehmensrichtlinien und die damit verbundenen Berechtigungsprüfungen nutzen.

Ausführliche Informationen zum Behavior Driven Governance finden Sie im *One Identity Manager Administrationshandbuch für Behavior Driven Governance*.

Detaillierte Informationen zum Thema

- [Automatische Attestierung von Richtlinienverletzungen konfigurieren](#) auf Seite 56
- [Attestierung von Richtlinienverletzungen starten](#) auf Seite 57

Automatische Attestierung von Richtlinienverletzungen konfigurieren

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

Für die Attestierung von Richtlinienverletzungen wird eine zur Unternehmensrichtlinie passende Attestierungsrichtlinie benötigt. Diese Attestierungsrichtlinie muss dieselben Objekte ermitteln, wie die Unternehmensrichtlinie.

Um die automatische Attestierung von Richtlinienverletzungen einzurichten

1. Erstellen Sie eine Attestierungsrichtlinie, die für die Attestierung von Objekten genutzt werden soll, welche eine Unternehmensrichtlinie verletzen. Stellen Sie sicher, dass durch diese Attestierungsrichtlinie und durch die Unternehmensrichtlinie die gleichen Objekte ermittelt werden.

Ausführliche Informationen zum Erstellen und Bearbeiten von Attestierungsrichtlinien finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*.

2. Erstellen Sie eine neue Unternehmensrichtlinie oder bearbeiten Sie eine bestehende Unternehmensrichtlinie. Erfassen Sie folgende Daten:

- **Attestierungsrichtlinie:** Wählen Sie aus der Auswahlliste die Attestierungsrichtlinie, die für die Attestierung von Richtlinienverletzungen genutzt werden soll.

WICHTIG: Stellen Sie sicher, dass durch diese Attestierungsrichtlinie und durch die Unternehmensrichtlinie die gleichen Objekte ermittelt werden. Prüfen Sie die zugeordneten Tabellen und Bedingungen.

- **Attestierung für neue Richtlinienverletzungen sofort starten:** Legen Sie fest, ob für jede neue Richtlinienverletzung sofort ein Attestierungsvorgang erstellt werden soll.

Wenn die Option deaktiviert ist, wird die Attestierung nur durch den an der Attestierungsrichtlinie hinterlegten Zeitplan gestartet.

Detaillierte Informationen zum Thema

- [Unternehmensrichtlinien erstellen und bearbeiten](#) auf Seite 11
- [Allgemeine Stammdaten für Unternehmensrichtlinien](#) auf Seite 12
- [Automatische Attestierung von Richtlinienverletzungen](#) auf Seite 56
- [Attestierung von Richtlinienverletzungen starten](#) auf Seite 57
- [Fehler bei der Attestierung von Richtlinienverletzungen](#) auf Seite 58

Attestierung von Richtlinienverletzungen starten

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

Es gibt verschiedene Möglichkeiten, um die Attestierung von Richtlinienverletzungen zu starten:

- Neue Richtlinienverletzungen sofort attestieren

Wenn an der Unternehmensrichtlinie **Attestierung für neue Richtlinienverletzungen sofort starten** aktiviert ist, wird bei der Richtlinienprüfung für jede neue Richtlinienverletzung sofort ein Attestierungsvorgang erstellt. Bei jedem Insert in die Tabelle `QERPolicyHasObject` wird dafür der Prozess `POL_QERPolicyHasObject_create_attestationcase` ausgeführt.

- Attestierung für alle Richtlinienverletzungen manuell starten

Um eine Attestierung aller Objekte zu veranlassen, welche eine Unternehmensrichtlinie verletzen, führen Sie im Manager die Aufgabe **Attestierungsvorgänge jetzt erstellen** aus.

- Attestierung für alle Richtlinienverletzungen zeitgesteuert starten

Die Attestierung wird regelmäßig durch den an der Attestierungsrichtlinie hinterlegten Zeitplan gestartet.

Der Prozess `POL_QERPolicyHasObject_create_attestationcase` prüft, ob alle betroffenen Objekte durch die zugeordnete Attestierungsrichtlinie als Attestierungsobjekte ermittelt werden können. Ist das nicht der Fall, erhält der Prozessschritt den Ausführungsstatus **Frozen** und es wird eine Fehlermeldung protokolliert.

Detaillierte Informationen zum Thema

- [Automatische Attestierung von Richtlinienverletzungen](#) auf Seite 56
- [Fehler bei der Attestierung von Richtlinienverletzungen](#) auf Seite 58
- [Attestierungsvorgänge erstellen](#) auf Seite 28

Fehler bei der Attestierung von Richtlinienverletzungen

Der Prozess (`POL_QERPolicyHasObject_create_attestationcase`), der die automatische Attestierung von Richtlinienverletzungen ausführt, scheitert und erhält den Ausführungsstatus **Frozen**.

Fehlermeldung: There are 1 objects that do not match to the attestation policy condition. (...)

Wahrscheinliche Ursache

Objekte, welche die Unternehmensrichtlinie verletzen, werden nicht als Attestierungsobjekte ermittelt. Möglicherweise wurde die Bedingung an der Unternehmensrichtlinie oder an der Attestierungsrichtlinie geändert.

Lösung

Stellen Sie sicher, dass durch die Attestierungsrichtlinie und durch die Unternehmensrichtlinie die gleichen Objekte ermittelt werden. Prüfen Sie die zugeordneten Tabellen und Bedingungen.

1. Öffnen Sie im Manager die Unternehmensrichtlinie.
2. Prüfen Sie die Basistabelle und die Bedingung.
3. Öffnen Sie im Manager die Attestierungsrichtlinie, die der Unternehmensrichtlinie zugeordnet ist.
4. Prüfen Sie die Bedingung und das zugeordnete Attestierungsverfahren.
5. Korrigieren Sie die Bedingungen oder zugeordneten Tabellen so, dass durch beide Richtlinien die gleichen Objekte ermittelt werden.

Ausführliche Informationen zur Bearbeitung von Attestierungsrichtlinien finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*.

Verwandte Themen

- [Allgemeine Stammdaten für Unternehmensrichtlinien](#) auf Seite 12
- [Automatische Attestierung von Richtlinienverletzungen](#) auf Seite 56

Risikomindernde Maßnahmen für Unternehmensrichtlinien

Für Unternehmen kann die Verletzung von regulatorischen Anforderungen unterschiedliche Risiken bergen. Um diese Risiken zu bewerten, können an Unternehmensrichtlinien Risikoindizes angegeben werden. Diese Risikoindizes geben darüber Auskunft, wie riskant eine Verletzung der jeweiligen Richtlinie für das Unternehmen ist. Sobald die Risiken erkannt und bewertet sind, können dafür risikomindernde Maßnahmen festgelegt werden.

Risikomindernde Maßnahmen sind unabhängig von den Funktionen des One Identity Manager. Sie werden nicht durch den One Identity Manager überwacht.

Risikomindernde Maßnahmen beschreiben Maßnahmen, die umgesetzt werden sollen, wenn eine Unternehmensrichtlinie verletzt wurde. Nach Umsetzung der Maßnahmen sollte die nächste Richtlinienprüfung keine Richtlinienverletzung ermitteln.

Um risikomindernde Maßnahmen zu bearbeiten

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | CalculateRiskIndex** und kompilieren Sie die Datenbank.

Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL-Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.


Ausführliche Informationen zur Risikobewertung finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.

Verwandte Themen

- [Risikomindernde Maßnahmen für Unternehmensrichtlinien erstellen und bearbeiten](#) auf Seite 61
- [Unternehmensrichtlinien an risikomindernde Maßnahmen zuweisen](#) auf Seite 61
- [Risikominderung für Unternehmensrichtlinien berechnen](#) auf Seite 62
- [Überblick über risikomindernde Maßnahmen anzeigen](#)

Risikomindernde Maßnahmen für Unternehmensrichtlinien erstellen und bearbeiten

Um risikomindernde Maßnahmen zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Risikoindex-Berechnungsvorschriften > Risikomindernde Maßnahmen**.
2. Wählen Sie in der Ergebnisliste eine risikomindernde Maßnahme und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
- ODER -
Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der risikomindernden Maßnahme.
4. Speichern Sie die Änderungen.

Für eine risikomindernde Maßnahme erfassen Sie folgende Stammdaten.

Tabelle 14: Allgemeine Stammdaten einer risikomindernden Maßnahme

Eigenschaft	Beschreibung
Maßnahme	Eindeutige Bezeichnung der risikomindernden Maßnahme.
Signifikanzminderung	Wert, um den das Risiko gesenkt wird, wenn die risikomindernde Maßnahme umgesetzt wird. Erfassen Sie eine Zahl zwischen 0 und 1.
Beschreibung	Ausführliche Beschreibung der risikomindernden Maßnahme.
Unternehmensbereich	Unternehmensbereich, in dem die risikomindernde Maßnahme angewendet werden soll.
Abteilung	Abteilung, in der die risikomindernde Maßnahme angewendet werden soll.

Unternehmensrichtlinien an risikomindernde Maßnahmen zuweisen

Mit dieser Aufgabe legen Sie fest, für welche Unternehmensrichtlinien eine risikomindernde Maßnahme gilt. Auf dem Zuweisungsformular können Sie nur die Arbeitskopien der Unternehmensrichtlinien zuweisen.


Um Unternehmensrichtlinien an risikomindernde Maßnahmen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Risikoindex-Berechnungsvorschriften > Risikomindernde Maßnahme**.
2. Wählen Sie in der Ergebnisliste die risikomindernde Maßnahme.
3. Wählen Sie die Aufgabe **Unternehmensrichtlinien zuweisen**.

Weisen Sie im Bereich **Zuordnungen hinzufügen** die Unternehmensrichtlinien zu.

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

Um eine Zuweisung zu entfernen

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

Risikominderung für Unternehmensrichtlinien berechnen

Die Signifikanzminderung einer risikomindernden Maßnahme gibt den Wert an, um den sich der Risikoindex einer Unternehmensrichtlinie reduziert, wenn die Maßnahme umgesetzt wird. Auf Basis des erfassten Risikoindex und der Signifikanzminderung errechnet der One Identity Manager einen reduzierten Risikoindex. Der One Identity Manager liefert Standard-Berechnungsvorschriften für die Berechnung der reduzierten Risikoindezes. Diese Berechnungsvorschriften können mit den One Identity Manager-Werkzeugen nicht bearbeitet werden.

Der reduzierte Risikoindex berechnet sich aus dem Risikoindex der Unternehmensrichtlinie und der Summe der Signifikanzminderungen aller zugewiesenen risikomindernden Maßnahmen.

$$\text{Risikoindex (reduziert)} = \text{Risikoindex} - \text{Summe der Signifikanzminderungen}$$

Wenn die Summe der Signifikanzminderung größer als der Risikoindex ist, wird der reduzierte Risikoindex auf den Wert 0 gesetzt.

Überblick über risikomindernde Maßnahmen für Unternehmensrichtlinien anzeigen

Auf dem Überblicksformular erhalten Sie auf einen Blick die wichtigsten Informationen zu einer risikomindernden Maßnahme.

Um einen Überblick über eine risikomindernde Maßnahme zu erhalten

1. Wählen Sie im Manager die Kategorie **Risikoindex-Berechnungsvorschriften > Risikomindernde Maßnahmen**.
2. Wählen Sie in der Ergebnisliste die risikomindernde Maßnahme.
3. Wählen Sie die Aufgabe **Überblick über die risikomindernde Maßnahme**.

Konfigurationsparameter für Unternehmensrichtlinien

Mit der Installation des Moduls sind zusätzliche Konfigurationsparameter im One Identity Manager verfügbar. Einige allgemeine Konfigurationsparameter sind für Unternehmensrichtlinien relevant. Die folgende Tabelle enthält eine Zusammenstellung aller für Unternehmensrichtlinien geltenden Konfigurationsparameter.

Tabelle 15: Übersicht der Konfigurationsparameter

Konfigurationsparameter	Bedeutung
QER Policy	<p>Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Überprüfung von Unternehmensrichtlinien. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren.</p> <p>Ist der Parameter aktiviert, können Sie die Modellbestandteile nutzen.</p> <p>Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL-Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im <i>One Identity Manager Konfigurationshandbuch</i>.</p>
QER Policy EmailNotification	<p>Die Parameter zur Mailbenachrichtigung werden verwendet.</p> <p>Unterhalb des Parameters werden die Informationen zur Benachrichtigung während der Überprüfung von Unternehmensrichtlinien definiert.</p>
QER Policy EmailNotification DefaultSenderAddress	<p>Standard E-Mail-Adresse des Absenders zum Versenden von automatisch generierten Benachrichtigungen bei der Überprüfung von Unternehmensrichtlinien. Ersetzen Sie den Standardwert durch eine gültige E-Mail-Adresse.</p>

Konfigurationsparameter	Bedeutung
QER CalculateRiskIndex	<p>Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Berechnung des Risikoindex. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren.</p> <p>Ist der Parameter aktiviert, können Werte für den Risikoindex erfasst und berechnet werden.</p> <p>Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL-Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im <i>One Identity Manager Konfigurationshandbuch</i>.</p>

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

A

- Administrator 7
- aktivieren
 - Unternehmensrichtlinie 24
- Anwendungsrolle 7
 - Attestierer 38
 - Richtlinienverantwortlicher 39
- Arbeitskopie (Unternehmensrichtlinie) 11
 - aktivieren 11, 19
 - erstellen 11, 25
 - kopieren 19
 - mit Richtlinie vergleichen 18
 - risikomindernde Maßnahme zuweisen 23
 - Überblicksformular 23
- Attestierer 7, 12, 38
- Attestierung
 - Objekte mit Richtlinienverletzung 56
- Attestierungsrichtlinie 12
- Ausnahmegenehmiger 7, 12
 - benachrichtigen 53
 - Identitäten zuweisen 21, 27
- Ausnahmegenehmigung begründen 42

B

- Basistabelle 12
- Bedingung 12
 - anzeigen 20, 26
 - ausblenden 20, 26
- Begründung 42
- Behavior Driven Governance 56

- Benachrichtigung
 - Mailvorlage 45

C

- Compliance Framework 31
 - Überblicksformular 33
 - Unternehmensrichtlinien zuweisen 32
- zuweisen 22

D

- deaktivieren 12
 - Unternehmensrichtlinie 24

M

- Maildefinition 44
- Mailvorlage
 - Basisobjekt 45
 - Hyperlink 47

O

- Objekte mit Richtlinienverletzung 20, 26
 - Attestierung starten 28, 57

R

- Richtlinie
 - aktivieren 24
 - deaktivieren 24
 - kopieren 25

- löschen 30
- Richtliniengruppe 30
 - zuweisen 12
- Richtlinienprüfung
 - starten 50
 - zeitgesteuert 50
- Richtlinienverantwortliche 7, 39
 - Identitäten zuweisen 22, 27
- Richtlinienverletzung
 - attestieren 28, 56-57
 - Attestierung konfigurieren 56
 - Ausnahmegenehmiger benachrichtigen 53
 - Ausnahmegenehmigung 51
 - Benachrichtigung 52
 - berechnen 49
 - E-Mail-Adresse 52
 - Entscheidungsstatus 55
 - ermitteln 50
 - ermittelte Objekte 20, 26
 - rezertifizieren 56
 - Richtlinienverantwortlichen benachrichtigen 54
- Risikobewertung
 - Unternehmensrichtlinie 15
- Risikoindex 15
 - berechnen 62
 - reduziert
 - berechnen 62
- Risikomindernde Maßnahme 60
 - erfassen 61
 - Signifikanzminderung 61
 - Überblick 62
 - Unternehmensrichtlinie zuweisen 61
 - zuweisen 23

S

- Schweregrad 15
- Signifikanzminderung 61
- Standardbegründung 42
 - Nutzungstyp 43
- Standard-Unternehmensrichtlinie 29
- Status 17

T

- Transparenzindex 15

U

- Überblicksformular 23, 29
- Unternehmensrichtlinie überprüfen 49

V

- Verantwortlicher 12
 - benachrichtigen 54
- Version 12

Z

- Zeitplan 33, 50
 - Richtlinienprüfung 33
 - sofort starten 38
 - Überblicksformular 38
 - Unternehmensrichtlinie zuweisen 37
 - zuweisen 17