One Identity Manager 8.1.4

Administrationshandbuch für Unternehmensrichtlinien

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 - 19. Oktober 2020, 08:29 Uhr
Version - 8.1.4

Inhalt

1

Unternehmensrichtlinien

Tabelle 1: Allgemeine Konfigurationsparameter für Unternehmensrichtlinien

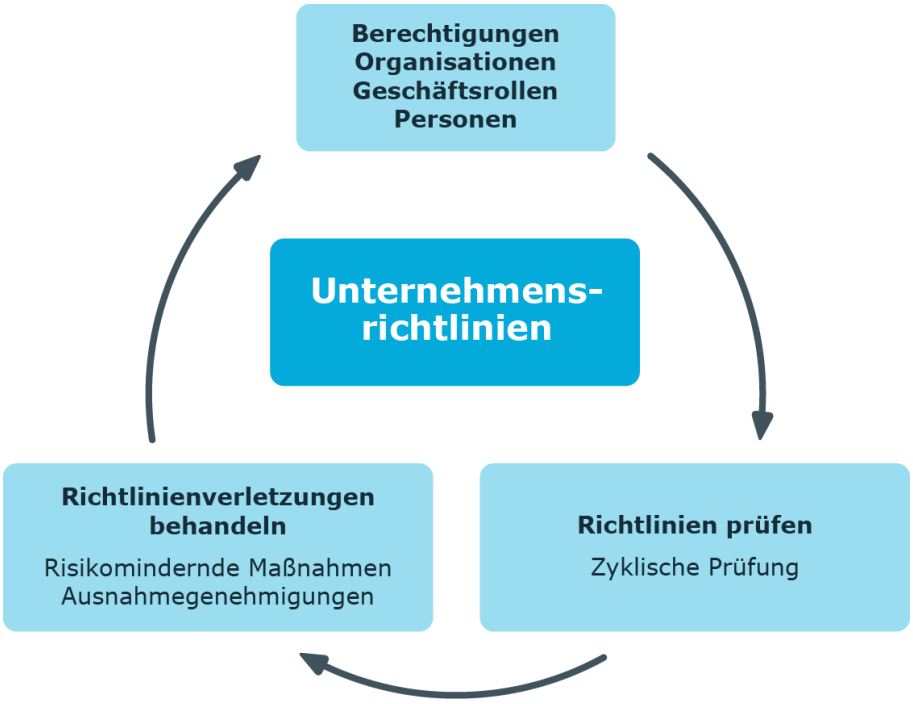
Konfigurationsparameter	Bedeutung
QER\Policy	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Überprüfung von Unternehmensrichtlinien. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Sie die Modellbestandteile nutzen.

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.

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.

Abbildung 1: Unternehmensrichtlinien im One Identity Manager



Beispiele für Unternehmensrichtlinien sind:

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

Um Unternehmensrichtlinien abbilden zu können

- Aktivieren Sie im Designer den Konfigurationsparameter "QER\Policy".

One Identity Manager Benutzer für Unternehmensrichtlinien

In die Verwaltung von Unternehmensrichtlinien sind folgende Benutzer eingebunden.

Tabelle 2: Benutzer

Benutzer	Aufgaben
Administratoren für Unternehmensrichtlinien	Die Administratoren müssen der Anwendungsrolle **Identity & Access Governance | Unternehmensrichlinien | Administratoren** zugewiesen sein.

Benutzer	Aufgaben
	Benutzer mit dieser Anwendungsrolle: • Erstellen die Basisdaten für die Erstellung der Unternehmensrichtlinien. • Erstellen die Richtlinien und weisen die Richtlinienverantwortlichen zu. • 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	Die Richtlinienverantwortlichen müssen der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Richtlinienverantwortliche** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • 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	• Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter.

Benutzer	Aufgaben
	• Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.
Ausnahmegenehmiger	Die Ausnahmegenehmiger müssen der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Ausnahmegenehmiger** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Bearbeiten die Richtlinienverletzungen. • Können Ausnahmegenehmigungen erteilen oder entziehen.
Attestierer für Unternehmensrichtlinien	Die Attestierer müssen der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Attestierer** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Attestieren im Web Portal die Unternehmensrichtlinien und Ausnahmegenehmigungen, für die sie verantwortlich sind. • Können die Stammdaten der Unternehmensrichtlinien sehen, aber nicht bearbeiten. HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.
Compliance & Security Officer	Compliance & Security Officer müssen der Anwendungsrolle **Identity & Access Governance | Compliance & Security Officer** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sehen im Web Portal alle Compliance-relevanten Informationen und deren Auswertungen. Dazu gehören Attestierungsrichtlinien, Unternehmensrichtlinien und Richtlinienverletzungen, Complianceregeln und Regelverletzungen sowie Risikoindex-Berechnungsvorschriften. • Können Attestierungsrichtlinien bearbeiten.
Auditoren	Die Auditoren sind der Anwendungsrolle **Identity & Access Governance | Auditoren** zugewiesen.

Benutzer	Aufgaben
	Benutzer mit dieser Anwendungsrolle: • Sehen im Web Portal alle für ein Audit relevanten Daten.

Basisdaten für Unternehmensrichtlinien

Um Unternehmensrichtlinien zu erstellen, Richtlinienprüfungen zu veranlassen und Richtlinienverletzungen zu behandeln, werden verschiedene Basisdaten benötigt.

Richtliniengruppen	Richtliniengruppen auf Seite 9
Compliance Frameworks	Compliance Frameworks auf Seite 10
Zeitpläne	Zeitpläne für die Richtlinienprüfung auf Seite 12
Attestierer	Attestierer auf Seite 16
Richtlinienverantwortliche	Richtlinienverantwortliche auf Seite 17
Ausnahmegenehmiger	Ausnahmegenehmiger auf Seite 19
Standardbegründungen	Standardbegründungen auf Seite 20

Richtliniengruppen

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

Um eine Richtliniengruppe zu bearbeiten

1. Wählen Sie die Kategorie **Unternehmensrichtlinien | Basisdaten zur Konfiguration | Richtliniengruppen**.
2. Wählen Sie in der Ergebnisliste eine Richtliniengruppe. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Für eine Richtliniengruppe erfassen Sie folgende Stammdaten.

Tabelle 3: Allgemeine Stammdaten einer Richtliniengruppe

Eigenschaft	Beschreibung
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.

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 bearbeiten

1. Wählen Sie 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 **Neu**.
3. Bearbeiten Sie die Stammdaten des Compliance Frameworks.
4. Speichern Sie die Änderungen.

Für Compliance Frameworks erfassen Sie folgende Eigenschaften.

Tabelle 4: 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 Frame-

Eigenschaft	Beschreibung
	works hierarchisch zu organisieren.
Verantwortliche	Anwendungsrolle, deren Mitglieder alle Unternehmensrichtlinien bearbeiten dürfen, die diesem Compliance Framework zugeordnet sind.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Zusätzliche Aufgaben für Compliance Frameworks

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

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

Überblick über das Compliance Framework

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

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**.

Unternehmensrichtlinien zuweisen

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

Um Unternehmensrichtlinien an Compliance Frameworks zuzuweisen

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 **Unternehmensrichtlinien zuweisen**.
4. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die Unternehmensrichtlinien, die zugewiesen werden sollen.

   – ODER –

Doppelklicken Sie im Bereich **Zuordnungen entfernen** auf die Unternehmensrichtlinien, deren Zuweisung entfernt werden soll.

5. Speichern Sie die Änderungen.

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 bearbeiten

1. Wählen Sie 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 5: 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	Angabe, ob der Zeitplan aktiv ist. HINWEIS: Nur Zeitpläne, die aktiv sind, werden ausgeführt.
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:

Eigenschaft	Bedeutung
	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. • 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. Als Intervalltypen sind **minütlich**, **stündlich**, **täglich**, **wöchentlich**, **monatlich** und **jährlich** zulässig. Für den Intervalltyp **wöchentlich** legen Sie den genauen Wochentag fest. Für den Intervalltyp **monatlich** legen Sie den Tag des Monats fest (1.-31. Tag eines Monats). Für den Intervalltyp **jährlich** legen Sie den Tag des Jahres fest (1. bis 366.Tag eines Jahres). HINWEIS: Würde bei Intervalltyp **monatlich** mit der Angabe des Subintervalls **29**, **30** oder **31** die Ausführung des Zeitplans erst im Folgemonat erfolgen, so wird der letzte Tag des aktuellen 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. Zeitpläne mit dem Intervalltyp **jährlich** und dem Subintervall **366** werden nur in Schaltjahren ausgeführt.
Startzeit	Feste Startzeit für die Intervalltypen **täglich**, **wöchentlich**, **monatlich** und **jährlich**. Geben Sie die Uhrzeit in der Ortszeit der ausgewählten Zeitzone an. Für die Intervalltypen **minütlich** und **stündlich** wird der Startzeitpunkt aus der Ausführungsfrequenz und dem Intervalltyp berechnet.
Wiederholen alle	Ausführungsfrequenz, mit welcher der zeitgesteuerte Auftrag

Eigenschaft	Bedeutung
	innerhalb des gewählten Zeitintervalls ausgeführt werden soll. Für den Intervalltyp **wöchentlich** wählen Sie mindestens einen Wochentag.
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.

Standardzeitpläne

Der One Identity Manager liefert standardmäßig folgende Zeitpläne für die Richtlinienprüfung aus.

Tabelle 6: Standardzeitpläne

Zeitplan	Beschreibung
default schedule policies	Standardzeitplan für die Richtlinienprüfung. Dieser Zeitplan erzeugt in regelmäßigen Abständen für jede Unternehmensrichtlinie einen Verarbeitungsauftrag für den DBQueue Prozessor zur Richtlinienprüfung.

Verwandte Themen

- Berechnen der Richtlinienverletzungen auf Seite 38

Zusätzliche Aufgaben für Zeitpläne

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

Überblick zum Zeitplan

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

Unternehmensrichtlinien zuweisen

Über diese Aufgabe weisen Sie dem ausgewählten Zeitplan die Unternehmensrichtlinien zu, die mit diesem Zeitplan ausgeführt werden sollen. Standardmäßig wird einer Unternehmensrichtlinien der Zeitplan "default schedule policies" zugewiesen. Über das Zuordnungsformular können Sie den ausgewählten Zeitplan an beliebige Unternehmensrichtlinien zuweisen.

Um den Zeitplan an Unternehmensrichtlinien zuzuweisen

1. Wählen Sie die Kategorie **Unternehmensrichtlinien | Basisdaten zur Konfiguration | Zeitpläne**.
2. Wählen Sie in der Ergebnisliste den Zeitplan.
3. Wählen Sie die Aufgabe **Unternehmensrichtlinien zuweisen**.
4. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die Unternehmensrichtlinien, die zugewiesen werden sollen.
5. Speichern Sie die Änderungen.

Um eine Zuordnung zu ändern

1. Wählen Sie 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.

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

Verwandte Themen

- Arbeitskopie aktivieren auf Seite 31
- Standardzeitpläne auf Seite 14
- Erweiterte Angaben zur Unternehmensrichtlinie auf Seite 26

Zeitplan sofort ausführen

Um einen Zeitplan sofort zu starten

1. Wählen Sie 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.

Attestierer

Installierte Module: Modul Attestierung

An Unternehmensrichtlinien können Personen zugewiesen werden, die als verantwortliche Attestierer für Attestierungsvorgänge herangezogen werden können. Dazu ordnen Sie in den allgemeinen Stammdaten einer Unternehmensrichtlinie eine Anwendungsrolle für Attestierer zu. Dieser Anwendungsrolle weisen Sie die Personen zu, die berechtigt sind, die Gültigkeit dieser Unternehmensrichtlinie zu attestieren.

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 7: Standardanwendungsrolle für Attestierer

Benutzer	Aufgaben
Attestierer für Unternehmensrichtlinien	Die Attestierer müssen der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Attestierer** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Attestieren im Web Portal die Unternehmensrichtlinien und Ausnahmegenehmigungen, für die sie verantwortlich sind. • Können die Stammdaten der Unternehmensrichtlinien

Benutzer	Aufgaben
	sehen, aber nicht bearbeiten. HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.

Um Attestierer zu bearbeiten

1. Wählen Sie die Kategorie **Unternehmensrichtlinien | Basisdaten zur Konfiguration | Attestierer**.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Wählen Sie in der Ergebnisliste eine Anwendungsrolle aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Anwendungsrolle.

Eigenschaft	Wert
Übergeordnete Anwendungsrolle	Ordnen Sie die Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Attestierer** oder eine untergeordnete Anwendungsrolle zu.

4. Speichern Sie die Änderungen.
5. Wählen Sie die Aufgabe **Personen zuweisen**, um Mitglieder in die Anwendungsrolle aufzunehmen.
6. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

   - ODER -

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

Richtlinienverantwortliche

An Unternehmensrichtlinien können Personen 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 8: Standardanwendungsrolle für Regelverantwortliche

Benutzer	Aufgaben
Richtlinienverantwortliche	Die Richtlinienverantwortlichen müssen der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Richtlinienverantwortliche** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • 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 Richtlinienverantwortliche zu bearbeiten

1. Wählen Sie die Kategorie **Unternehmensrichtlinien | Basisdaten zur Konfiguration | Richtlinienverantwortliche**.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Wählen Sie in der Ergebnisliste eine Anwendungsrolle aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Anwendungsrolle.

Eigenschaft	Wert
Übergeordnete Anwendungsrolle	Ordnen Sie die Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Richtlinienverantwortliche** oder eine untergeordnete Anwendungsrolle zu.

4. Speichern Sie die Änderungen.
5. Wählen Sie die Aufgabe **Personen zuweisen**, um Mitglieder in die Anwendungsrolle aufzunehmen.
6. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

   - ODER -

Entfernen Sie im Bereich **Zuordnungen entfernen** die Personen.

7. Speichern Sie die Änderungen.

Ausnahmegenehmiger

An Unternehmensrichtlinien können Personen 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 9: Standardanwendungsrolle für Ausnahmegenehmiger

Benutzer	Aufgaben
Ausnahmegenehmiger	Die Ausnahmegenehmiger müssen der Anwendungsrolle **Identity & Access Governance | Unternehmensrichtlinien | Ausnahmegenehmiger** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Bearbeiten die Richtlinienverletzungen. • Können Ausnahmegenehmigungen erteilen oder entziehen.

Um Ausnahmegenehmiger zu bearbeiten

1. Wählen Sie die Kategorie **Unternehmensrichtlinien | Basisdaten zur Konfiguration | Ausnahmegenehmiger**.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Wählen Sie in der Ergebnisliste eine Anwendungsrolle aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Anwendungsrolle.

Eigenschaft	Wert
Übergeordnete	Ordnen Sie die Anwendungsrolle **Identity & Access Gover-**

Eigenschaft	Wert
Anwendungsrolle	**nance | Unternehmensrichtlinien | Ausnah-megenehmiger** oder eine untergeordnete Anwendungsrolle zu.

4. Speichern Sie die Änderungen.
5. Wählen Sie die Aufgabe **Personen zuweisen**, um Mitglieder in die Anwendungsrolle aufzunehmen.
6. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

   - ODER -

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

Verwandte Themen

- Erteilen einer Ausnahmegenehmigung auf Seite 40

Standardbegründungen

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 bearbeiten

1. Wählen Sie 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 10: Allgemeine Stammdaten einer Standardbegründung

Eigenschaft	Beschreibung
Standardbegründung	Begründungstext, so wie er im Web Portal angezeigt werden soll.

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

Vordefinierte Standardbegründungen

Der One Identity Manager liefert vordefinierte Standardbegründungen aus. Diese Standardbegründungen werden bei automatischen Entscheidungen durch den One Identity Manager an der Richtlinienverletzung eingetragen.

Um vordefinierte Standardbegründungen anzuzeigen

- Wählen Sie die Kategorie **Unternehmensrichtlinien | Basisdaten | Standardbegründungen | Vordefiniert**.

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.

Erstellen und Bearbeiten von Unternehmensrichtlinien

Für jede Unternehmensrichtlinie wird in der Datenbank eine Arbeitskopien angelegt. Um Unternehmensrichtlinien zu erstellen und zu ändern, bearbeiten Sie deren Arbeitskopien.

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 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 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 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 einer Unternehmensrichtlinie

Für eine Unternehmensrichtlinie erfassen Sie die folgenden Stammdaten.

Tabelle 11: Allgemeine Stammdaten einer Unternehmensrichtlinie

Eigenschaft	Beschreibung
Richtlinie	Bezeichnung der Unternehmensrichtlinie.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Hauptversionsnummer	Bearbeitungsstand der Unternehmensrichtlinie als Versionsnummern. Bei jeder Änderung der Bedingung wird in der Standardinstallation des One Identity Manager die letzte Stelle der Versionsnummer erhöht.
Arbeitskopie	Angabe, ob es sich um die Arbeitskopie der Unternehmensrichtlinie handelt.
Deaktiviert	Angabe, 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	Angabe, ob Ausnahmegenehmigungen erlaubt sind, wenn die Unternehmensrichtlinie verletzt wird. Zuweisungen, die eine Richtlinienverletzung verursachen, können somit trotzdem genehmigt und zugewiesen werden.
Ausnahmegenehmiger	Anwendungsrolle, deren Mitglieder berechtigt sind, Ausnahmegenehmigungen für Verletzungen dieser Unternehmensrichtlinie zu erteilen. Um eine neue Anwendungsrolle zu erstellen, klicken Sie .

Eigenschaft	Beschreibung
	Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Hinweise zur Ausnahmegenehmigung	Informationen, die Ausnahmegenehmiger für ihre Entscheidung benötigen. Diese Hinweise sollten die Risiken und Nebenwirkungen einer Ausnahmegenehmigung beschreiben.
Attestierer	Anwendungsrolle, deren Mitglieder berechtigt sind, Attestierungsvorgänge über Unternehmensrichtlinien und Richtlinienverletzungen zu entscheiden. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Ohne Bedingung	Angabe, ob die Unternehmensrichtlinie keinen direkten Bezug zum One Identity Manager-Datenmodell hat. Wenn die Option aktiviert ist, wird die Schaltfläche **Bedingung bearbeiten...** deaktiviert. Wenn die Option deaktiviert ist, muss eine Bedingung formuliert werden, die alle Objekte ermittelt, welche die Unternehmensrichtlinie verletzen.
Basistabelle	Basistabelle, auf die sich die Unternehmensrichtlinie bezieht. Ausgehend von dieser Tabelle, werden die Objekte 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

- Richtlinie aktivieren und deaktivieren auf Seite 34
- Richtliniengruppen auf Seite 9
- Richtlinienverantwortliche auf Seite 17
- Ausnahmegenehmiger auf Seite 19
- Attestierer auf Seite 16
- Bedingung anzeigen auf Seite 31

Verwandte Themen

- One Identity Manager Anwenderhandbuch für die Benutzeroberfläche der One Identity Manager-Werkzeuge

Risikobewertung

Tabelle 12: Konfigurationsparameter für die Risikobewertung

Konfigurationsparameter	Wirkung bei Aktivierung
QER\CalculateRiskIndex	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Berechnung des Risikoindex. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Werte für den Risikoindex erfasst und berechnet werden.

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.

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

Tabelle 13: 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 wird die Werteliste {Niedrig, Mittel, Hoch, Kritisch} angezeigt.
Risikoindex	Gibt an, wie riskant Verletzungen dieser Unternehmensrichtlinien für das Unternehmen sind. Stellen Sie über den Schieberegler einen

Eigenschaft	Beschreibung
	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 für die originale Unternehmensrichtlinie berechnet. Um diesen Wert in die Arbeitskopie zu übernehmen, führen Sie die Aufgabe **Arbeitskopie erstellen** aus. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter "QER\CalculateRiskIndex" aktiviert ist. 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
Max. Anzahl Regelverletzungen	Anzahl der Richtlinienverletzungen, die für diese Unternehmensrichtlinie zugelassen sind.

Detaillierte Informationen zum Thema

- Risikomindernde Maßnahmen auf Seite 50
- One Identity Manager Administrationshandbuch für Risikobewertungen
- Report Editor im One Identity Manager Konfigurationshandbuch

Verwandte Themen

- Arbeitskopie erstellen auf Seite 34

Erweiterte Angaben zur Unternehmensrichtlinie

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

Tabelle 14: 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 "default schedule policies" zugeordnet. Sie können hier einen eigenen Zeitplan zuordnen.

Verwandte Themen

- Berechnen der Richtlinienverletzungen auf Seite 38

Richtlinienvergleich

Die Ergebnismengen einer Arbeitskopie und der originalen Unternehmensrichtlinie können in einem Vergleich gegenübergestellt werden. Auf dem Tabreiter **Richtlinienvergleich** des Stammdatenformulars der Arbeitskopie werden daraufhin die Vergleichswerte dargestellt.

Tabelle 15: Ergebnis des Richtlinienvergleichs

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

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.

Detaillierte Informationen zum Thema

- Arbeitskopie und Original einer Unternehmensrichtlinie vergleichen auf Seite 32

Standard-Unternehmensrichtlinien

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 die Kategorie **Unternehmensrichtlinien | Richtlinien | Arbeitskopien von Richtlinien | Vordefiniert**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Arbeitskopie aktivieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **OK**.

Für Standard-Unternehmensrichtlinien können folgende Eigenschaften unternehmensspezifisch geändert werden:

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

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

Zusätzliche Aufgaben für Arbeitskopien

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

Überblick über die Arbeitskopie

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

Compliance Framework 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 die Kategorie **Unternehmensrichtlinien | Richtlinien | Arbeitskopien von Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Compliance Frameworks zuweisen**.
4. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die Compliance Frameworks, die zugewiesen werden sollen.

   – ODER –

   Doppelklicken Sie im Bereich **Zuordnungen entfernen** auf die Compliance Frameworks, deren Zuweisung entfernt werden soll.
5. Speichern Sie die Änderungen.

Risikomindernde Maßnahmen 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 die Kategorie **Unternehmensrichtlinien | Richtlinien | Arbeitskopien von Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Risikomindernde Maßnahmen zuweisen**.
4. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die risikomindernden Maßnahmen, die zugewiesen werden sollen.

   – ODER –

   Doppelklicken Sie im Bereich **Zuordnungen entfernen** auf die risikomindernden Maßnahmen, deren Zuweisung entfernt werden soll.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Risikomindernde Maßnahmen auf Seite 50

Ausnahmegenehmiger pflegen

Über diese Aufgabe können Sie die Ausnahmegenehmiger für die ausgewählte Unternehmensrichtlinie pflegen. Personen 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 Personen als Ausnahmegenehmiger zu berechtigen

1. Wählen Sie die Kategorie **Unternehmensrichtlinien | Richtlinien | Arbeitskopien von Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Ausnahmegenehmiger pflegen**.
4. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die Personen, die der Anwendungsrolle zugewiesen werden sollen.

   – ODER –

   Doppelklicken Sie im Bereich **Zuordnungen entfernen** auf die Personen, deren Zuweisung entfernt werden soll.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten einer Unternehmensrichtlinie auf Seite 23
- Ausnahmegenehmiger auf Seite 19

Richtlinienverantwortliche pflegen

Über diese Aufgabe können Sie die Richtlinienverantwortlichen für die ausgewählte Unternehmensrichtlinie pflegen. Personen 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 Personen als Richtlinienverantwortliche zu berechtigen

1. Wählen Sie die Kategorie **Unternehmensrichtlinien | Richtlinien | Arbeitskopien von Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Verantwortliche pflegen**.
4. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die Personen, die der Anwendungsrolle zugewiesen werden sollen.

– ODER –

Doppelklicken Sie im Bereich **Zuordnungen entfernen** auf die Personen, deren Zuweisung entfernt werden soll.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten einer Unternehmensrichtlinie auf Seite 23
- Richtlinienverantwortliche auf Seite 17

Arbeitskopie 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 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.

Bedingung 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 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 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**.

Richtlinie kopieren

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

Um eine Arbeitskopie zu kopieren

1. Wählen Sie 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**.

Arbeitskopie und Original einer Unternehmensrichtlinie 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.

Um eine Unternehmensrichtlinie mit der Arbeitskopie zu vergleichen

1. Wählen Sie 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**.

Tabelle 16: Ergebnis des Richtlinienvergleichs

Richtlinienverletzungen	Es werden alle Personen 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

- Richtlinienvergleich auf Seite 27

Zeige ausgewählte Objekte

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 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.

Zusätzliche Aufgaben für Unternehmensrichtlinien

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

Überblick über die Unternehmensrichtlinie

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 die Kategorie **Unternehmensrichtlinien | Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Überblick über die Richtlinie**.

Arbeitskopie 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 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.

Richtlinie aktivieren und deaktivieren

Damit Richtlinienverletzungen für eine Unternehmensrichtlinie ermittelt werden können, aktivieren Sie die Unternehmensrichtlinie. Um Unternehmensrichtlinien von der Richtlinienprüfung auszuschließen, können Sie sie 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 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 die Kategorie **Unternehmensrichtlinien | Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Richtlinie deaktivieren**.

Bedingung 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 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 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**.

Richtlinie kopieren

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

Um eine Unternehmensrichtlinie zu kopieren

1. Wählen Sie 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**.

Zeige ausgewählte Objekte

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 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.

Neu berechnen

An einer Unternehmensrichtlinie stehen verschiedene Aufgaben zur Ermittlung der Richtlinienverletzungen zur Verfügung. Weitere Informationen finden Sie unter Überprüfen der Unternehmensrichtlinien auf Seite 38.

Ausnahmegenehmiger pflegen

Über diese Aufgabe können Sie die Ausnahmegenehmiger für die ausgewählte Unternehmensrichtlinie pflegen. Personen 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 Personen als Ausnahmegenehmiger zu berechtigen

1. Wählen Sie die Kategorie **Unternehmensrichtlinien | Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Ausnahmegenehmiger pflegen**.
4. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die Personen, die der Anwendungsrolle zugewiesen werden sollen.

   – ODER –

   Doppelklicken Sie im Bereich **Zuordnungen entfernen** auf die Personen, deren Zuweisung entfernt werden soll.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten einer Unternehmensrichtlinie auf Seite 23
- Ausnahmegenehmiger auf Seite 19

Richtlinienverantwortliche pflegen

Über diese Aufgabe können Sie die Richtlinienverantwortlichen für die ausgewählte Unternehmensrichtlinie pflegen. Personen 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 Personen als Richtlinienverantwortliche zu berechtigen

1. Wählen Sie die Kategorie **Unternehmensrichtlinien | Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Unternehmensrichtlinie.
3. Wählen Sie die Aufgabe **Verantwortliche pflegen**.
4. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die Personen, die der Anwendungsrolle zugewiesen werden sollen.

   – ODER –

   Doppelklicken Sie im Bereich **Zuordnungen entfernen** auf die Personen, deren Zuweisung entfernt werden soll.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten einer Unternehmensrichtlinie auf Seite 23
- Richtlinienverantwortliche auf Seite 17

Löschen von Unternehmensrichtlinien

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 Revisionssicherheit) aufbewahren wollen.

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

Um eine Unternehmensrichtlinie zu löschen:

1. Wählen Sie 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.

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.

Berechnen der 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.

Zeitgesteuerte Richtlinienprüfung

Für die komplette Überprüfung aller Unternehmensrichtlinien ist in der One Identity Manager-Standardinstallation der Zeitplan "default schedule policies" 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 12
- Richtlinie aktivieren und deaktivieren auf Seite 34

Ad-hoc-Richtlinienprüfung

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

Tabelle 17: Zusätzliche Aufgaben einer Unternehmensrichtlinie

Aufgabe	Beschreibung
Richtlinie neu berechnen	Die ausgewählte Unternehmensrichtlinie wird sofort überprüft.
Alles neu berechnen	Alle Unternehmensrichtlinien werden sofort überprüft.

Berichte über Richtlinienverletzungen

Der 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 18: 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 • Richtlinienverletzungen, über die noch entschieden werden muss, • Richtlinienverletzungen ohne Ausnahmegenehmigung, • Richtlinienverletzungen mit Ausnahmegenehmigung.

Bericht	Beschreibung
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 einer Ausnahmegenehmigung

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.

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 Personen zugewiesen.

Um Ausnahmegenehmigungen zu erteilen, nutzen Sie das Web Portal.

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 einer Unternehmensrichtlinie auf Seite 23
- One Identity Manager Anwenderhandbuch für das Web Portal

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 Benachrichtigungen im Bestellprozess zu nutzen

1. Stellen Sie sicher, dass das E-Mail-Benachrichtungssystem im One Identity Manager konfiguriert ist. Ausführliche Informationen finden Sie im *One Identity Manager 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 Personen eine Standard-E-Mail-Adresse besitzen. An diese E-Mail Adresse werden die Benachrichtigungen versendet. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.
5. Stellen Sie sicher, dass für alle Personen eine Sprachkultur ermittelt werden kann. Nur so erhalten die Personen die E-Mail Benachrichtigungen in ihrer Sprache. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.
6. Konfigurieren Sie die Benachrichtigungsverfahren.

Verwandte Themen

- Unternehmensspezifische Mailvorlagen für Benachrichtigungen erstellen auf Seite 44

Aufforderung zur Ausnahmegenehmigung

Tabelle 19: Konfigurationsparameter für Benachrichtigungen über Richtlinienverletzungen

Konfigurationsparameter	Bedeutung bei Aktivierung
QER\Policy\EmailNotification\NewExceptionApproval	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, wenn eine Ausnahmegenehmigung für eine neue Richtlinienverletzung erforderlich ist.

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

Voraussetzungen

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

Um Aufforderungen zur Ausnahmegenehmigung zu versenden

- Aktivieren Sie im Designer den Konfigurationsparameter "QER\Policy\EmailNotification\NewExceptionApproval".

  Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage "Richtlinien - Neue Ausnahmegenehmigung erforderlich" an alle Ausnahmegenehmiger versendet.

TIPP: Um eine andere als die Standardmailvorlage für diese Benachrichtigungen zu nutzen, ändern Sie den Wert des Konfigurationsparameters.

Benachrichtigung über Richtlinienverletzungen ohne Ausnahmegenehmigung

Tabelle 20: Konfigurationsparameter für Benachrichtigungen über Richtlinienverletzungen

Konfigurationsparameter	Bedeutung bei Aktivierung
QER\Policy\EmailNotification\NotPermittedViolation	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, wenn eine

Konfigurationsparameter	Bedeutung bei Aktivierung
	neue unzulässige Richtlinienverletzung auftritt.

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

Voraussetzungen

- An der Unternehmensrichtlinie ist die Option **Ausnahmegenehmigung möglich** deaktiviert.
- Der Unternehmensrichtlinie ist eine Anwendungsrolle für **Verantwortliche** zugeordnet.
- Dieser Anwendungsrolle sind Personen zugewiesen.

Um Richtlinienverantwortliche über Richtlinienverletzungen zu informieren

- Aktivieren Sie im Designer den Konfigurationsparameter "QER\Policy\EmailNotification\NotPermittedViolation".

  Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage "Richtlinien - Unzulässige Verletzung aufgetreten" an alle Richtlinienverantwortlichen versendet.

TIPP: Um eine andere als die Standardmailvorlage für diese Benachrichtigungen zu nutzen, ändern Sie den Wert des Konfigurationsparameters.

Entscheidungsstatus einer Richtlinienverletzung

Richtlinienverletzungen bearbeiten Sie mit dem Web Portal. Darüber hinaus können Sie 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 das Formularelement für die Richtlinienverletzung und blenden Sie die Listeneinträge ein.
2. 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 die Unternehmensrichtlinie auf Seite 33

Unternehmensspezifische Mailvorlagen für Benachrichtigungen erstellen

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.

Zur einfachen Erstellung von Benachrichtigungen ist im One Identity Manager ein Mailvorlageneditor integriert. Mit dem Mailvorlageneditor können Sie Mailtexte im WYSIWYG-Modus erstellen und bearbeiten.

Um Mailvorlagen 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**.

Allgemeine Eigenschaften einer Mailvorlage

Für eine Mailvorlage werden die folgenden allgemeinen Eigenschaften abgebildet.

Tabelle 21: Eigenschaften einer Mailvorlage

Eigenschaft	Bedeutung
Mailvorlage	Bezeichnung der Mailvorlage. Mit dieser Bezeichnung werden die Mailvorlagen in den Administrationswerkzeugen und im Web Portal angezeigt. Übersetzen Sie den eingegebenen Text über die Schaltfläche .
Basisobjekt	Basisobjekt der Mailvorlage. Die Angabe eines Basisobjekts ist nur erforderlich, wenn in der Maildefinition Eigenschaften des Basisobjekts referenziert werden. Für Benachrichtigungen über Richtlinienverletzungen verwenden Sie die Basisobjekte `QERPolicy` oder `QERPolicyHasObject`.
Bericht (Parametersatz)	Bericht, der über die Mailvorlage zur Verfügung gestellt wird.
Beschreibung	Beschreibung der Mailvorlage. Übersetzen Sie den eingegebenen Text

Eigenschaft	Bedeutung
	über die Schaltfläche  .
Zielformat	Format, in dem die E-Mail Benachrichtigung generiert wird. Zulässige Werte sind: • **HTML**: Die E-Mail Benachrichtigung wird als HTML formatiert. Im HTML-Format können Textformatierungen wie beispielsweise unterschiedliche Schriftarten, farbige Schriften oder andere Textformatierungen enthalten sein. • **TXT**: Die E-Mail Benachrichtigung wird als Text formatiert. Das Text-Format unterstützt keine fetten, kursiven oder farbige Schriften oder andere Textformatierungen. Bilder, die direkt in der Benachrichtigung angezeigt werden, werden ebenfalls nicht unterstützt.
Designtyp	Design, in welchem die E-Mail Benachrichtigung generiert wird. Zulässige Werte sind: • **Mailvorlage**: Die generierte E-Mail Benachrichtigung enthält den Mailbody entsprechend der Maildefinition. • **Bericht**: Die generierte E-Mail Benachrichtigung enthält den unter **Bericht (Parametersatz)** angegebenen Bericht als Mailbody. • **Mailvorlage, Bericht im Anhang**: Die generierte E-Mail Benachrichtigung enthält den Mailbody entsprechend der Maildefinition. Der unter **Bericht (Parametersatz)** angegebene Bericht wird als PDF-Datei an die Benachrichtigung angehängt.
Wichtigkeit	Wichtigkeit für die E-Mail Benachrichtigung. Zulässig sind die Werte **Niedrig**, **Normal** und **Hoch**.
Vertraulichkeit	Vertraulichkeit für die E-Mail Benachrichtigung. Zulässig sind die Werte **Normal**, **Persönlich**, **Privat** und **Vertraulich**.
Abbestellen erlaubt	Angabe, ob ein Empfänger die E-Mail Benachrichtigung abbestellen kann. Ist die Option aktiviert, kann die E-Mail Benachrichtigung über das Web Portal abbestellt werden.
Deaktiviert	Angabe, ob diese Mailvorlage deaktiviert ist.
Maildefinition	Eindeutige Bezeichnung der Maildefinition.
Sprachkultur	Sprachkultur, für welche die Mailvorlage gelten soll. Bei Generierung einer E-Mail-Benachrichtigung werden die Spracheinstellungen des Empfängers berücksichtigt.
Betreff	Betreff der E-Mail Benachrichtigung.
Mailbody	Inhalt der E-Mail Benachrichtigung.

Erstellen und Bearbeiten einer Maildefinition

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.

Um eine neue Maildefinition zu erstellen

1. Öffnen Sie die Mailvorlage im Mailvorlageneditor.
2. Klicken Sie die Schaltfläche neben der Auswahlliste **Maildefinition**.
3. Wählen Sie in der Auswahlliste **Sprachkultur** 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. Öffnen Sie die Mailvorlage im Mailvorlageneditor.
2. Wählen Sie in der Auswahlliste **Maildefinition** die Sprache.
3. Bearbeiten Sie die Betreffzeile und den Mailbody.
4. Speichern Sie die Änderungen.

Eigenschaften des Basisobjekts verwenden

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 finden Sie im *One Identity Manager Konfigurationshandbuch*.

Verwenden von Hyperlinks zum Web Portal

Tabelle 22: Konfigurationsparameter für die URL zum Web Portal

Konfigurationsparameter	Wirkung bei Aktivierung
QER\WebPortal\BaseURL	URL zum Web Portal. Diese Adresse wird in Mailvorlagen genutzt, um Hyperlinks auf das Web Portal einzufügen.

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 den URL-Pfad zum Web Portal. Den Konfigurationsparameter bearbeiten Sie im Designer.

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

  mit:

  `<Servername> = Name des Servers`

  `<Anwendung> = Pfad zum Web Portal 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:

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

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 23: Funktionen des Skriptes `VI_BuildComplianceLinks`

Funktion	Verwendung
VI_BuildQERPolicyLink_Show	Öffnet die Seite zur Ausnahmegenehmigung im Web Portal.

Anpassen der E-Mail Signatur

Die E-Mail Signatur für die Mailvorlagen konfigurieren Sie über die folgenden Konfigurationsparameter. Die Konfigurationsparameter bearbeiten Sie im Designer.

Tabelle 24: Konfigurationsparameter für die E-Mail Signatur

Konfigurationsparameter	Beschreibung
Common | MailNotification | Signature	Angaben zur Signatur in automatisch aus Mailvorlagen generierten E-Mails.
Common | MailNotification | Signature | Caption	Unterschrift unter die Grußformel.
Common | MailNotification | Signature | Company	Name des Unternehmens.
Common | MailNotification | Signature | Link	Link zur Firmenwebseite.
Common | MailNotification | Signature | LinkDisplay	Anzeigetext für den Link zur Firmenwebseite.

Das Skript `VI_GetRichMailSignature` stellt die Bestandteile einer E-Mail Signatur entsprechend der Konfigurationsparameter zur Verwendung in Mailvorlagen zusammen.

Risikomindernde Maßnahmen

Tabelle 25: Konfigurationsparameter für die Risikobewertung

Konfigurationsparameter	Wirkung bei Aktivierung
QER\CalculateRiskIndex	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Berechnung des Risikoindex. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Werte für den Risikoindex erfasst und berechnet werden.

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.

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

Stammdaten erfassen

Um risikomindernde Maßnahmen 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 26: 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.

Zusätzliche Aufgaben für risikomindernde Maßnahmen

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

Überblick über die risikomindernde Maßnahme

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**.

Unternehmensrichtlinien 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 die Kategorie **Risikoindex-Berechnungsvorschriften | Risikomindernde Maßnahme**.
2. Wählen Sie in der Ergebnisliste die risikomindernde Maßnahme.
3. Wählen Sie die Aufgabe **Unternehmensrichtlinien zuweisen**.
4. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die Unternehmensrichtlinien, die zugewiesen werden sollen.

   - ODER -

   Doppelklicken Sie im Bereich **Zuordnungen entfernen** auf die Unternehmensrichtlinien, deren Zuweisung entfernt werden soll.
5. Speichern Sie die Änderungen.

Risikominderung 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 Risikoindizes. 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.

```
Risikoindex (reduziert) = Risikoindex - Summe der Signifikanzminderungen
```

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

Anhang A

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 27: Übersicht der Konfigurationsparameter

Konfigurationsparameter	Bedeutung
QER\Policy	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Überprüfung von Unternehmensrichtlinien. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Sie die Modellbestandteile nutzen.
QER\Policy\EmailNotification	Die Parameter zur Mailbenachrichtigung werden verwendet. Unterhalb des Parameters werden die Informationen zur Benachrichtigung während der Überprüfung von Unternehmensrichtlinien definiert.
QER\Policy\EmailNotification\DefaultSenderAddress	Der Konfigurationsparameter enthält die Absender E-Mail Adresse für automatisch generierte Nachrichten innerhalb der Überprüfung von Unter-

Konfigurationsparameter	Bedeutung
	nehmensrichtlinien.
QER\Policy\EmailNotification\NewExceptionApproval	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, wenn eine Ausnahmegenehmigung für eine neue Richtlinienverletzung erforderlich ist.
QER\Policy\EmailNotification\NotPermittedViolation	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, wenn eine neue unzulässige Richtlinienverletzung auftritt.
QER\CalculateRiskIndex	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Berechnung des Risikoindex. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Werte für den Risikoindex erfasst und berechnet werden.

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

Index

S

T

U

V

Z