One Identity Manager 8.2

Administrationshandbuch für Complianceregeln

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.

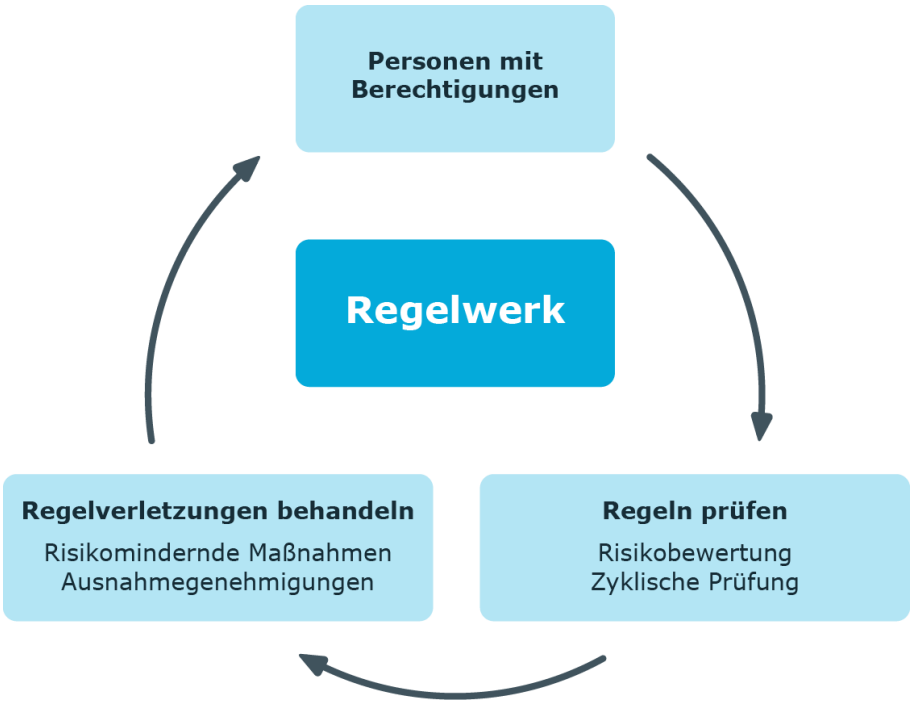
One Identity Manager Administrationshandbuch für Complianceregeln
Aktualisiert - 24. November 2021, 10:39 Uhr
Version - 8.2

Inhalt

Complianceregeln und Identity Audit

Mit dem One Identity Manager können Regeln zur Einhaltung und Überwachung regulatorischer Anforderungen definiert und Regelverletzungen automatisiert behandelt werden. Complianceregeln definieren, welche Berechtigungen oder Berechtigungskombinationen im Rahmen des Identity Audit für die Personen im Unternehmen überprüft werden sollen. Durch die Regelprüfung können einerseits bestehende Regelverletzungen gefunden werden. Andererseits können mögliche Regelverletzungen präventiv identifiziert und damit vermieden werden.

Abbildung 1: Identity Audit im One Identity Manager



Einfache Beispiele für Regeln sind:

- Eine Person darf nicht gleichzeitig zwei Berechtigungen A und B erhalten.
- Nur Personen einer bestimmten Abteilung dürfen eine bestimmte Berechtigung besitzen.
- Jedem Benutzerkonto muss eine verantwortliche Person zugeordnet sein.

Mit der Identity Audit Funktion des One Identity Manager können Sie:

- Regeln über beliebige Zuweisungen an Personen definieren
- Risiken möglicher Regelverletzungen bewerten
- Risikomindernde Maßnahmen festlegen
- Regelmäßige oder spontane Regelprüfungen veranlassen
- Bearbeitungsberechtigungen von Personen innerhalb eines SAP Mandanten detailliert überprüfen (mittels SAP Funktionen)
- Regelverletzungen nach verschiedenen Kriterien auswerten
- Berichte über Regeln und Regelverletzungen erstellen

Auf Basis dieser Informationen können Sie Korrekturen an den Daten im One Identity Manager vornehmen und in die angeschlossenen Zielsysteme übertragen. Durch die im One Identity Manager integrierte Berichtsfunktion können die Informationen für entsprechende Prüfungen bereitgestellt werden.

Um die Identity Audit Funktion zu nutzen

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

One Identity Manager Benutzer für das Identity Audit

In die Verwaltung des Regelwerks und die Bearbeitung von Regelverletzungen sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Administratoren für	Die Administratoren müssen der Anwendungsrolle **Identity &**

Benutzer	Aufgaben
Identity Audit	**Access Governance | Identity Audit | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Erstellen die Basisdaten für die Erstellung des Regelwerks. • Erstellen die Complianceregeln und weisen die Regelverantwortlichen zu. • Können bei Bedarf die Regelprüfung starten und Regelverletzungen einsehen. • Erstellen Berichte über Regelverletzungen. • Erfassen risikomindernde Maßnahmen. • Erstellen und bearbeiten Risikoindex-Berechnungsvorschriften. • Überwachen die Identity Audit Funktionen. • Administrieren die Anwendungsrollen für Regelverantwortliche, Ausnahmegenehmiger und Attestierer. • Richten bei Bedarf weitere Anwendungsrollen ein.
Regelverantwortliche	Die Regelverantwortlichen müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Regelverantwortliche** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind inhaltlich verantwortlich für Complianceregeln, beispielsweise Wirtschaftsprüfer oder Revisionsabteilung. • Bearbeiten die Arbeitskopien der Complianceregeln, denen die Anwendungsrolle zugeordnet ist. • Aktivieren und deaktivieren Complianceregeln. • Können bei Bedarf die Regelprüfung starten und Regelverletzungen einsehen. • Weisen risikomindernde Maßnahmen zu.
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den

Benutzer	Aufgaben
	Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne.
Ausnahmegenehmiger	Die Ausnahmegenehmiger müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Ausnahmegenehmiger** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Bearbeiten im Web Portal die Regelverletzungen. • Können im Web Portal Ausnahmegenehmigungen erteilen oder entziehen.
Attestierer für Complianceregeln	Die Attestierer müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Attestierer** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Attestieren im Web Portal die Complianceregeln und Ausnahmegenehmigungen, für die sie verantwortlich sind. • Können die Stammdaten der Complianceregeln 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.

Benutzer	Aufgaben
Auditoren	Die Auditoren sind der Anwendungsrolle **Identity & Access Governance | Auditoren** zugewiesen. Benutzer mit dieser Anwendungsrolle: • Sehen im Web Portal alle für ein Audit relevanten Daten.

Basisdaten für die Regelerstellung

Um Regeln zu erstellen, Regelprüfungen zu veranlassen und Regelverletzungen zu behandeln, werden verschiedene Basisdaten benötigt.

Regelgruppen:	Regelgruppen auf Seite 10
Compliance Frameworks:	Compliance Frameworks auf Seite 12
Zusatzeigenschaften:	Zusatzeigenschaften und Eigenschaftengruppen auf Seite 19
Zeitpläne:	Zeitpläne für die Regelprüfung auf Seite 13
Unternehmensbereiche:	Unternehmensbereiche auf Seite 24
Attestierer:	Attestierer für Complianceregeln auf Seite 26
Regelverantwortliche:	Regelverantwortliche auf Seite 27
Ausnahmegenehmiger:	Ausnahmegenehmiger auf Seite 28
Standardbegründungen:	Standardbegründungen für Regelverletzungen auf Seite 29
Mailvorlagen:	Mailvorlagen für das Identity Audit bearbeiten auf Seite 76

Regelgruppen

Regelgruppen verwenden Sie zur funktionalen Zusammenfassung von Regeln, beispielsweise zur Gruppierung von Kontenrichtlinien oder zur Abgrenzung von Funktionen ("Segregation of duties").

Um eine Regelgruppe zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Regelgruppen**.
2. Wählen Sie in der Ergebnisliste eine Regelgruppe. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Klicken Sie in der Ergebnisliste .

3. Bearbeiten Sie die Stammdaten der Regelgruppe.
4. Speichern Sie die Änderungen.

Für eine Regelgruppe erfassen Sie folgende Stammdaten.

Tabelle 2: Eigenschaften einer Regelgruppe

Eigenschaft	Beschreibung
Name der Gruppe	Bezeichnung der Regelgruppe.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Übergeordnete Gruppe	Übergeordnete Regelgruppe in einer Hierarchie. Wählen Sie aus der Auswahlliste die übergeordnete Regelgruppe, um Regelgruppen hierarchisch zu organisieren.

Complianceregeln an Regelgruppen zuweisen

Über diese Aufgabe legen Sie fest, welche Complianceregeln zur ausgewählten Regelgruppe gehören.

Um Complianceregeln an eine Regelgruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Regelgruppen**.
2. Wählen Sie in der Ergebnisliste die Regelgruppe.
3. Wählen Sie die Aufgabe **Regeln zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Complianceregeln zu.

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

   Um eine Zuweisung zu entfernen

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

Überblick über Regelgruppen anzeigen

Auf dem Überblicksformular erhalten Sie auf einen Blick die wichtigsten Informationen zu einer Regelgruppe. Im Bericht **Überblick der Regelverletzungen** erhalten Sie eine Zusammenfassung über alle Regelverletzungen einer Regelgruppe.

Um einen Überblick über eine Regelgruppe zu erhalten

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Regelgruppen**.
2. Wählen Sie in der Ergebnisliste die Regelgruppe.
3. Wählen Sie die Aufgabe **Überblick über die Regelgruppe**.

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 **Identity Audit > 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 3: 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 Complianceregeln bearbeiten dürfen, die diesem Compliance Framework zugeordnet sind.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Complianceregeln an Compliance Frameworks zuweisen

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

Um Complianceregeln an Compliance Frameworks zuzuweisen

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

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Complianceregel 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 Regelverletzungen** erhalten Sie eine Zusammenfassung über alle Regelverletzungen eines Compliance Frameworks.

Um einen Überblick über ein Compliance Framework zu erhalten

1. Wählen Sie im Manager die Kategorie **Identity Audit > 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 Regelprüfung

Die zyklische komplette Überprüfung aller Regeln wird über Zeitpläne gesteuert. Der One Identity Manager stellt zwei Standardzeitpläne für die Regelprüfung bereit. Diese sorgen dafür, dass die Hilfstabellen für die Objektzuordnungen regelmäßig aktualisiert werden und die Regelprüfung gestartet wird. Dafür können Sie weitere Zeitpläne einrichten. Stellen Sie sicher, dass diese Zeitpläne den Regeln zugewiesen sind.

Um Zeitpläne zu erstellen oder zu bearbeiten

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

   In der Ergebnisliste werden alle Zeitpläne angezeigt, die für die Tabelle `ComplianceRule` konfiguriert sind.
2. Wählen Sie in der Ergebnisliste einen Zeitplan. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   – 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 4: 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 nur 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. • 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

Eigenschaft	Bedeutung
	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.
	• **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.
	  • 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.

Eigenschaft	Bedeutung

- 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.

- **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

Eigenschaft	Bedeutung
	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.

Standardzeitpläne für das Identity Audit

Der One Identity Manager stellt standardmäßig folgende Zeitpläne für das Identity Audit bereit.

Tabelle 5: Standardzeitpläne

Zeitplan	Beschreibung
Berechnung der Complianceregeln (`default schedule compliance rule check`)	Standardzeitplan für die Regelprüfung. Dieser Zeitplan erzeugt in regelmäßigen Abständen für jede Regel einen Verarbeitungsauftrag für den DBQueue Prozessor zur Regelprüfung.
Befüllung der Complianceregel Objekte (`default schedule compliance rule fill`)	Standardzeitplan zur Befüllung der Hilfstabellen. Für die Ermittlung potentieller Regelverletzungen im Web Portal werden Hilfstabellen für Objektzuordnungen ausgewertet. Diese Hilfstabellen werden regelmäßig durch den DBQueue Prozessor aktualisiert. Dieser Auftrag erzeugt zyklisch die Verarbeitungsaufträge zur Aktualisierung der Hilfstabellen.

Verwandte Themen

- Prüfen von Complianceregeln auf Seite 60
- Ermitteln potenzieller Regelverletzungen auf Seite 71

Complianceregeln an Zeitpläne zuweisen

Über diese Aufgabe weisen Sie dem ausgewählten Zeitplan die Complianceregeln zu, die mit diesem Zeitplan geprüft werden sollen. Standardmäßig werden einer Regel die Zeitpläne **Befüllung der Complianceregel Objekte** und **Berechnung der Complianceregeln** zugewiesen. Über die Zuordnungsformulare können Sie den ausgewählten Zeitplan an beliebige Regeln zuweisen.

Um den Zeitplan an Regeln zuzuweisen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Zeitpläne**.
2. Wählen Sie in der Ergebnisliste den Zeitplan.
3. Wählen Sie die Aufgabe **Regeln (zur Befüllung) zuweisen**.

   - ODER -

   Wählen Sie die Aufgabe **Regeln (zur Prüfung) zuweisen**.
4. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die Regeln, die zugewiesen werden sollen.
5. Speichern Sie die Änderungen.

Um eine Zuordnung zu ändern

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Zeitpläne**.
2. Wählen Sie in der Ergebnisliste den Zeitplan.
3. Wählen Sie die Aufgabe **Regeln (zur Befüllung) zuweisen**.

   - ODER -

   Wählen Sie die Aufgabe **Regeln (zur Prüfung) zuweisen**.
4. Wählen Sie im Kontextmenü des Zuordnungsformulars **Zeige bereits anderen Objekten zugewiesene Objekte**.

   Es werden die Regeln eingeblendet, die bereits anderen Zeitplänen zugewiesen sind.
5. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf eine dieser Regeln.

   Dieser Regel 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 Regeln eine Pflichteingabe.

Verwandte Themen

- Arbeitskopie aktivieren auf Seite 42
- Standardzeitpläne für das Identity Audit auf Seite 17

- Erweiterte Angaben für Complianceregeln auf Seite 36

Zeitpläne sofort ausführen

Um einen Zeitplan sofort zu starten

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

Zusatzeigenschaften und Eigenschaftengruppen

Um in der Regelbedingung auf Eigenschaften zuzugreifen, für die es keine direkte Abbildung im One Identity Manager-Datenmodell gibt, können Sie Zusatzeigenschaften verwenden. Je nach Umfang eines Regelwerkes kann es notwendig sein, eine große Anzahl an Zusatzeigenschaften zu pflegen. Zusatzeigenschaften fassen Sie daher über Eigenschaftengruppen zusammen.

Um Zusatzeigenschaften abzubilden

1. Richten Sie eine Eigenschaftengruppe ein, unter der die Zusatzeigenschaften zusammengefasst werden.
2. Unterhalb einer Eigenschaftengruppe richten Sie die Zusatzeigenschaften ein.
3. Weisen Sie die Zusatzeigenschaften an die Objekte zu.

   Es können beliebig viele Objekte der unterschiedlichen Objekttypen an eine Zusatzeigenschaft zugewiesen werden.

Eigenschaftengruppen für Zusatzeigenschaften erstellen

Eigenschaftengruppen werden genutzt, um Zusatzeigenschaften zu gruppieren. Jede Zusatzeigenschaft muss mindestens einer Eigenschaftengruppe zugeordnet sein. Darüber hinaus können die Zusatzeigenschaften beliebigen weiteren Eigenschaftengruppen zugewiesen sein.

Um eine Eigenschaftengruppe zu erstellen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Zusatzeigenschaften**.
2. Klicken Sie in der Ergebnisliste .
3. Erfassen Sie eine Bezeichnung und eine Beschreibung für die Eigenschaftengruppe.
4. Speichern Sie die Änderungen.

Zusatzeigenschaften erstellen und bearbeiten

Um eine Zusatzeigenschaft zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Zusatzeigenschaften > <Eigenschaftengruppe>**.
2. Wählen Sie in der Ergebnisliste eine Zusatzeigenschaft. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Stammdaten für Zusatzeigenschaften

Für eine Zusatzeigenschaft erfassen Sie die folgenden Stammdaten.

Tabelle 6: Stammdaten einer Zusatzeigenschaft

Eigenschaft	Beschreibung
Name der Zusatzeigenschaft	Bezeichnung der Zusatzeigenschaft.
Eigenschaftengruppe	Die Eigenschaftengruppen dienen zur Strukturierung der Zusatzeigenschaften. Zu einer Zusatzeigenschaft können Sie über das Stammdatenformular eine Eigenschaftengruppe zuweisen. Die

Eigenschaft	Beschreibung
	Zusatzeigenschaften werden in der Navigationsansicht nach dieser Eigenschaftengruppe gruppiert. Sollte die Zuordnung einer Zusatzeigenschaft zu mehreren Eigenschaftengruppen notwendig sein, so können Sie zusätzliche Eigenschaftengruppen zuweisen.
Untere Bereichsgrenze	Untere Bereichsgrenze zur weiteren Unterteilung.
Obere Bereichsgrenze	Obere Bereichsgrenze zur weiteren Unterteilung.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Verwandte Themen

- Bereichsgrenzen für Zusatzeigenschaften festlegen auf Seite 23
- Weitere Eigenschaftengruppen an Zusatzeigenschaften zuweisen auf Seite 22
- Zusatzeigenschaften an Eigenschaftengruppen zuweisen auf Seite 21

Zusatzeigenschaften an Eigenschaftengruppen zuweisen

Jede Zusatzeigenschaft muss mindestens einer Eigenschaftengruppe zugeordnet sein. Darüber hinaus können die Zusatzeigenschaften beliebigen weiteren Eigenschaftengruppen zugewiesen sein.

Sollen einer Eigenschaftengruppe weitere Zusatzeigenschaften zugewiesen werden, verwenden Sie die Aufgabe **Zusatzeigenschaften zuweisen**.

Um Zusatzeigenschaften an eine Eigenschaftengruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Zusatzeigenschaften**.
2. Wählen Sie in der Ergebnisliste eine Eigenschaftengruppe.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Zusatzeigenschaft und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Zusatzeigenschaften auf Seite 20
- Weitere Eigenschaftengruppen an Zusatzeigenschaften zuweisen auf Seite 22

Weitere Eigenschaftengruppen an Zusatzeigenschaften zuweisen

Jede Zusatzeigenschaft muss mindestens einer Eigenschaftengruppe zugeordnet sein. Darüber hinaus können die Zusatzeigenschaften beliebigen weiteren Eigenschaftengruppen zugewiesen sein. Sollte die Zuordnung einer Zusatzeigenschaft zu mehreren Eigenschaftengruppen notwendig sein, so können Sie über die Aufgabe **Eigenschaftengruppen zuweisen** zusätzliche Eigenschaftengruppen zuweisen.

Um eine Zusatzeigenschaft an Eigenschaftengruppen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Zusatzeigenschaften > <Eigenschaftengruppe>**.
2. Wählen Sie in der Ergebnisliste eine Zusatzeigenschaft.
3. Wählen Sie die Aufgabe **Eigenschaftengruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Eigenschaftengruppen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Eigenschaftengruppe und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Zusatzeigenschaften auf Seite 20
- Zusatzeigenschaften an Eigenschaftengruppen zuweisen auf Seite 21

Bereichsgrenzen für Zusatzeigenschaften festlegen

Über Bereichsgrenzen können Sie innerhalb der Zusatzeigenschaften eine weitere Unterteilung vornehmen. Die Angabe von Bereichsgrenzen für Zusatzeigenschaften ist nicht zwingend erforderlich. Wenn Sie eine untere Bereichsgrenze definieren, müssen Sie nicht unbedingt eine obere Bereichsgrenze festlegen. Wenn Sie jedoch eine obere Bereichsgrenze angeben, so müssen Sie auch eine untere Bereichsgrenze festlegen.

Bei der Definition von Bereichsgrenzen beachten Sie Folgendes:

- Grundsätzlich ist jede beliebige Zeichenkette als untere oder obere Bereichsgrenze zulässig.
- Als Platzhalter für beliebig viele (auch Null) Zeichen kann * verwendet werden.
- Platzhalter dürfen nur am Ende einer Zeichenkette stehen, beispielsweise AB*. Nicht zulässig ist beispielsweise *AB oder A*B.
- Wenn Sie die untere Bereichsgrenze ohne Platzhalter angeben, dann dürfen Sie auch für die obere Bereichsgrenze keinen Platzhalter verwenden.

Für die Zeichenkettenlänge gibt es folgende Einschränkungen:

- Wenn Sie die untere Bereichsgrenze und die obere Bereichsgrenze ohne Platzhalter eintragen, so müssen beide Zeichenketten gleich lang sein, beispielsweise untere Bereichsgrenze 123/obere Bereichsgrenze 456. Nicht zulässig ist beispielsweise untere Bereichsgrenze 123/obere Bereichsgrenze 45 oder untere Bereichsgrenze 123/obere Bereichsgrenze 4567.
- Wenn Sie in der unteren Bereichsgrenze einen Platzhalter verwenden und in der oberen Bereichsgrenzen keinen Platzhalter nutzen, dann muss die Zeichenkettenlänge der oberen Bereichsgrenze gleich oder größer der Zeichenkettenlänge der unteren Bereichsgrenze sein.
- Wenn Sie in der unteren Bereichsgrenze und in der oberen Bereichsgrenze einen Platzhalter verwenden, so müssen beide Zeichenketten gleich lang sein, beispielsweise untere Bereichsgrenze 123*/obere Bereichsgrenze 456*. Nicht zulässig sind beispielsweise untere Bereichsgrenze 123*/obere Bereichsgrenze 45* oder untere Bereichsgrenze 123*/obere Bereichsgrenze 4567*.

Überblick über Zusatzeigenschaften anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Zusatzeigenschaft. Dazu zählt die Zugehörigkeit der Zusatzeigenschaft zu den verschiedenen Objekten des One Identity Manager.

Um einen Überblick über eine Zusatzeigenschaft zu erhalten

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Zusatzeigenschaften > <Eigenschaftengruppe>**.
2. Wählen Sie in der Ergebnisliste die Zusatzeigenschaft.
3. Wählen Sie die Aufgabe **Überblick über die Zusatzeigenschaft**.

Um einen Überblick über eine Eigenschaftengruppe zu erhalten

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Zusatzeigenschaften**.
2. Wählen Sie in der Ergebnisliste die Eigenschaftengruppe.
3. Wählen Sie die Aufgabe **Überblick über die Eigenschaftengruppe**.

Objekte an Zusatzeigenschaften zuweisen

Zusatzeigenschaften können an Unternehmensressourcen, hierarchische Rollen und Personen zugewiesen werden.

Um eine Zusatzeigenschaft an Objekte zuzuweisen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Zusatzeigenschaften > <Eigenschaftengruppe>**.
2. Wählen Sie in der Ergebnisliste eine Zusatzeigenschaft.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Wählen Sie in der Auswahlliste **Tabelle** den gewünschten Objekttyp.

   Es werden die zum Objekttyp gehörigen Objekte auf dem Formular angezeigt.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Objekte zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Objekt und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Unternehmensbereiche

Um Regelprüfungen im Rahmen des Identity Audit für verschiedene Bereiche Ihres Unternehmens auswerten zu können, richten Sie Unternehmensbereiche ein. Unternehmensbereiche können an hierarchische Rollen und Leistungspositionen zugeordnet werden. Für die Unternehmensbereiche und die hierarchischen Rollen können Sie Kriterien erfassen, die Auskunft über das Risiko von Regelverletzungen geben. Dafür legen Sie fest,

wie viele Regelverletzungen in einem Unternehmensbereich oder einer Rolle zulässig sind. Für jede Rolle können Sie separate Bewertungskriterien erfassen, wie beispielsweise Risikoindex oder Transparenzindex.

Unternehmensbereiche können darüber hinaus bei der Entscheidung von Bestellungen oder Attestierungsvorgängen durch Peer-Gruppen-Analyse genutzt werden.

Beispiel: Einsatz von Unternehmensbereichen

Das Risiko von Regelverletzungen für Kostenstellen soll bewertet werden. Gehen Sie folgendermaßen vor:

1. Richten Sie Unternehmensbereiche ein.
2. Ordnen Sie die Unternehmensbereiche den Kostenstellen zu.
3. Definieren Sie Bewertungskriterien für die Kostenstellen.
4. Legen Sie die Anzahl zulässiger Regelverletzungen für die Unternehmensbereiche fest.
5. Weisen Sie die Unternehmensbereiche den Complianceregeln zu, die für die Auswertung relevant sind.
6. Erstellen Sie über die Berichtsfunktion des One Identity Manager einen Bericht, der das Ergebnis der Regelprüfung für die Unternehmensbereiche nach beliebigen Kriterien aufbereitet.

Um Unternehmensbereiche zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Unternehmensbereiche**.
2. Wählen Sie in der Ergebnisliste einen Unternehmensbereich und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Für einen Unternehmensbereich erfassen Sie folgende Stammdaten.

Tabelle 7: Eigenschaften von Unternehmensbereichen

Eigenschaft	Beschreibung
Unternehmensbereich	Bezeichnung des Unternehmensbereichs.
Überg. Unternehmensbereich	Übergeordneter Unternehmensbereich in einer Hierarchie. Wählen Sie aus der Auswahlliste den übergeordneten Unter-

Eigenschaft	Beschreibung
	nehmensbereich aus, um Unternehmensbereiche hierarchisch zu organisieren.
Max. Anzahl Regelverletzungen	Anzahl der Regelverletzungen, die in diesem Unternehmensbereich zulässig sind. Dieser Wert kann bei der Regelprüfung ausgewertet werden.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Attestierer für Complianceregeln

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

An Complianceregeln können Sie Personen zuweisen, die als verantwortliche Attestierer für Attestierungsvorgänge herangezogen werden können. Dazu ordnen Sie den Complianceregeln eine Anwendungsrolle für Attestierer zu. Dieser Anwendungsrolle weisen Sie die Personen zu, die berechtigt sind, die Gültigkeit dieser Complianceregel 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 Identity Audit	Die Attestierer müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Attestierer** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Attestieren im Web Portal die Complianceregeln und Ausnahmegenehmigungen, für die sie verantwortlich sind. • Können die Stammdaten der Complianceregeln sehen, aber nicht bearbeiten. HINWEIS: Diese Anwendungsrolle steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.

Um Personen in die Standardanwendungsrolle für Attestierer aufzunehmen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Attestierer**.
2. Wählen Sie die Aufgabe **Personen zuweisen**.

3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Person und doppelklicken Sie ✓.

4. Speichern Sie die Änderungen.

Regelverantwortliche

An Complianceregeln können Personen zugewiesen werden, die inhaltlich für die Regeln verantwortlich sind. Das können beispielsweise die Wirtschaftsprüfer oder die Revisionsabteilung sein. Dazu ordnen Sie den Complianceregeln eine Anwendungsrolle für Regelverantwortliche zu. Dieser Anwendungsrolle weisen Sie die Personen zu, die berechtigt sind, die Arbeitskopien der Complianceregeln zu bearbeiten.

Im One Identity Manager ist eine Standardanwendungsrolle für Regelverantwortliche 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
Regelverantwortliche	Die Regelverantwortlichen müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Regelverantwortliche** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind inhaltlich verantwortlich für Complianceregeln, beispielsweise Wirtschaftsprüfer oder Revisionsabteilung. • Bearbeiten die Arbeitskopien der Complianceregeln, denen die Anwendungsrolle zugeordnet ist. • Aktivieren und deaktivieren Complianceregeln. • Können bei Bedarf die Regelprüfung starten und Regelverletzungen einsehen. • Weisen risikomindernde Maßnahmen zu.

Um Personen in die Standardanwendungsrolle für Regelverantwortliche aufzunehmen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Regelverantwortliche**.
2. Wählen Sie die Aufgabe **Personen zuweisen**.
3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

   Um eine Zuweisung zu entfernen

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

Ausnahmegenehmiger

An Complianceregeln können Personen zugewiesen werden, die Ausnahmegenehmigungen für Regelverletzungen erteilen dürfen. Dazu ordnen Sie den Complianceregeln eine Anwendungsrolle für Ausnahmegenehmiger zu. Dieser Anwendungsrolle weisen Sie die Personen zu, die berechtigt sind, Ausnahmen für Regelverletzungen zu genehmigen.

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	Die Ausnahmegenehmiger müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Ausnahmegenehmiger** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Bearbeiten im Web Portal die Regelverletzungen. • Können im Web Portal Ausnahmegenehmigungen erteilen oder entziehen.

Um Personen in die Standardanwendungsrolle für Ausnahmegenehmiger aufzunehmen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Ausnahmegenehmiger**.
2. Wählen Sie die Aufgabe **Personen zuweisen**.

3. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Person und doppelklicken Sie .

4. Speichern Sie die Änderungen.

Verwandte Themen

- Erteilen einer Ausnahmegenehmigung auf Seite 66

Standardbegründungen für Regelverletzungen

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 Regelverletzung hinterlegen.

Um Standardbegründungen zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Identity Audit > 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 Regelverletzung eingetragen werden soll. Diese

Eigenschaft	Beschreibung
	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.

Verwandte Themen

- Vordefinierte Standardbegründungen für Regelverletzungen auf Seite 30

Vordefinierte Standardbegründungen für Regelverletzungen

Der One Identity Manager stellt vordefinierte Standardbegründungen bereit. Diese Standardbegründungen werden bei automatischen Entscheidungen durch den One Identity Manager an der Regelverletzung 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 **Identity Audit > 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 **Nutzungtyp** 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 Regelverletzungen auf Seite 29

Einrichten eines Regelwerkes

Regeln zur Einhaltung und Überwachung regulatorischer Anforderungen definieren Sie in einem Regelwerk. Eine Regel enthält im One Identity Manager neben der technischen Beschreibung auch weitere Eigenschaften, wie beispielsweise Schweregrad einer Regelverletzung, Eigentümer, Verantwortlicher oder Revisionsinformationen. Ebenso ist eine Klassifizierung der Regeln nach Kategorien (Compliance Frameworks) und Regelgruppen möglich.

Sobald eine Regel angelegt wird, wird in der Datenbank ein zugehöriges Objekt für Regelverletzungen erzeugt. In dieses Objekt werden alle Personen aufgenommen, die die Regel verletzen.

Complianceregeln erstellen und bearbeiten

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

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

Um eine neue Regel zu erstellen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln**.
2. Klicken Sie in der Ergebnisliste .
3. Erfassen Sie die Stammdaten der Regel.
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 Regel in der Datenbank angelegt. Die Arbeitskopie bleibt bestehen und wird für nachfolgende Regeländerungen genutzt.

Um eine bestehende Regel zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln**.
   a. Wählen Sie in der Ergebnisliste eine Regel.
   b. Wählen Sie die Aufgabe **Arbeitskopie erstellen**.

      Die Daten der bestehenden Arbeitskopie werden auf Nachfrage mit den Daten der originalen Regel überschrieben. Die Arbeitskopie wird geöffnet und kann bearbeitet werden.

- ODER -

Wählen Sie im Manager die Kategorie **Identity Audit > Regeln > Arbeitskopien von Regeln**.

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 Regel übertragen. Dabei wird eine deaktivierte Regel auf Nachfrage aktiviert.

Allgemeine Stammdaten für Complianceregeln

Für eine Regel erfassen Sie folgende allgemeine Stammdaten.

Tabelle 12: Allgemeine Stammdaten einer Regel

Eigenschaft	Beschreibung
Regel	Bezeichnung der Regel. Mit dieser Bezeichnung wird beim Erstellen einer neuen Regel automatisch ein neues Objekt für Regelverletzungen erzeugt. HINWEIS: Wenn Sie Complianceregeln umbenennen, wird die Bezeichnung der zugehörigen Regelverletzung nicht geändert.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Hauptversionsnummer	Bearbeitungsstand der Regel als Versionsnummer. Bei jeder Änderung der Regelbedingung wird in der Standardinstallation des One Identity Manager die letzte Stelle der Versionsnummer erhöht.
Arbeitskopie	Angabe, ob es sich um die Arbeitskopie der Regel handelt.
Deaktiviert	Angabe, ob die Regel deaktiviert ist. Nur aktivierte Regeln werden in der Regelprüfung berücksichtigt. Zur Aktivierung und Deaktivierung einer Regel verwenden Sie die Aufgaben **Regel aktivieren** und **Regel deaktivieren**. Die Arbeitskopie einer Regel ist immer deaktiviert.
Regelgruppe	Regelgruppe, zu der die Regel inhaltlich gehört. Wählen Sie eine Regelgruppe aus der Auswahlliste. Um eine neue Regelgruppe zu erstellen, klicken Sie . Erfassen Sie den Namen und eine Beschreibung der Regelgruppe.

Eigenschaft	Beschreibung
Regelverantwortliche	Anwendungsrolle, deren Mitglieder inhaltlich für die Regel 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 Regel verletzt wird. Zuweisungen oder Bestellungen, die eine Regelverletzung verursachen, können somit trotzdem genehmigt und zugewiesen werden.
Ausnahmegenehmiger	Anwendungsrolle, deren Mitglieder berechtigt sind, Ausnahmegenehmigungen für Verletzungen dieser Regel zu erteilen. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Mailvorlage neue Verletzung	Mailvorlage, die zur Generierung einer E-Mail verwendet wird, um Regelverantwortliche oder Ausnahmegenehmiger über neue Regelverletzungen zu informieren.
Hinweise zur Ausnahmegenehmigung	Informationen, die Ausnahmegenehmiger für ihre Entscheidung benötigen. Diese Hinweise sollten die Risiken und Nebenwirkungen einer Ausnahmegenehmigung beschreiben.
Max. Tage gültig	Gültigkeitszeitraum für Ausnahmegenehmigungen, um Ausnahmegenehmigungen zeitlich zu befristen. Erfassen Sie die Anzahl der Tage, die eine Ausnahmegenehmigung gelten darf. Nach Ablauf des Gültigkeitszeitraums werden die Ausnahmegenehmigungen automatisch aufgehoben.
Attestierer	Anwendungsrolle, deren Mitglieder berechtigt sind, Attestierungsvorgänge über Complianceregeln und Regelverletzungen zu entscheiden. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu. HINWEIS: Das Eingabefeld steht zur Verfügung, wenn das Modul Attestierung vorhanden ist.
Unternehmensbereich	Unternehmensbereich, für den die Regel relevant ist.
Abteilung	Abteilung, für welche die Regel relevant ist.
Regel für zyklische Prüfung und Risikobewertung im IT Shop	Angabe, ob die Regel bei der Risikobewertung von IT Shop Bestellungen berücksichtigt werden soll. Das Eingabefeld ist nur sichtbar, wenn der

Eigenschaft	Beschreibung
	Konfigurationsparameter **QER | ComplianceCheck | SimpleMode | NonSimpleAllowed** aktiviert ist.
Regel nur für zyklische Prüfung	Angabe, ob die Regel nur bei der zyklischen Regelprüfung berücksichtigt werden soll. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | ComplianceCheck | SimpleMode | NonSimpleAllowed** aktiviert ist.
Bedingung	Bedingungen, die zu einer Regelverletzung führen. Die Bedingungen stellen Sie über einen Regeleditor zusammen.

Detaillierte Informationen zum Thema

- Erstellen von Regelbedingungen auf Seite 48
- Complianceregeln aktivieren und deaktivieren auf Seite 46
- Regelgruppen auf Seite 10
- Regelverantwortliche auf Seite 27
- Ausnahmegenehmiger auf Seite 28
- Zeitliche Befristung von Ausnahmegenehmigungen auf Seite 67
- Attestierer für Complianceregeln auf Seite 26
- Unternehmensbereiche auf Seite 24
- Erstellen von Regelbedingungen auf Seite 48
- Regelbedingungen im erweiterten Modus auf Seite 56

Verwandte Themen

- Auswertung der Regelprüfung auf Seite 62
- Erteilen einer Ausnahmegenehmigung auf Seite 66
- Benachrichtigungen über Regelverletzungen ohne Ausnahmegenehmigung auf Seite 71
- Aufforderung zur Ausnahmegenehmigung auf Seite 70

Risikobewertung für Regelverletzungen

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

Der Risikoindex von Systemberechtigungen kann als Objekteigenschaft bereits beim Erstellen von Regelbedingungen berücksichtigt werden. Durch solche Regeln kann beispielsweise verhindert werden, dass Systemberechtigungen, die einen festgelegten Risikoindex übersteigen, im IT Shop bestellt werden können.

Um Objekte, Zuweisungen und Regelverletzungen 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 Regelverletzung im Rahmen des Identity Audits erfassen Sie auf dem Tabreiter **Bewertungskriterien** Werte für die Einstufung der Regel.

Tabelle 13: Bewertungskriterien einer Regel

Eigenschaft	Beschreibung
Schweregrad	Gibt an, welche Auswirkung Verletzungen dieser Regel für das Unternehmen haben. Stellen Sie über den Schieberegler einen Wert zwischen **0** und **1** ein. **0** ... keine Auswirkung **1** ... Jede Regelverletzung ist ein Problem.
Auswirkung	Gibt in verbaler Beschreibung an, welche Auswirkung Verletzungen dieser Regel für das Unternehmen haben. In der Standardinstallation werden die Werte **Niedrig**, **Mittel**, **Hoch** und **Kritisch** angezeigt.
Risikoindex	Gibt an, wie riskant Verletzungen dieser Regel für das Unternehmen sind. Abhängig vom Wert der Auswirkung wird per Bildungsregel ein Risikoindexwert vorgegeben. **Tabelle 14: Risikoindex in Abhängigkeit der Auswirkungen** **Auswirkung** / **Risikoindex** Niedrig / 0,0 Mittel / 0,33 Hoch / 0,66 Kritisch / 1,0 Dieser Wert kann geändert werden. Stellen Sie über den Schieberegler einen Wert zwischen **0** und **1** ein. **0** ... kein Risiko **1** ... Jede Regelverletzung ist ein Problem. Sobald sich die Auswirkung ändert, passt die Bildungsregel den Risikoindex wieder an. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter

Eigenschaft	Beschreibung
	QER | CalculateRiskIndex aktiviert ist.
Risikoindex (reduziert)	Gibt den Risikoindex unter Berücksichtigung der zugewiesenen risikomindernden Maßnahmen an. Der Risikoindex einer Regel wird um die Signifikanzminderung aller zugewiesenen risikomindernden Maßnahmen reduziert. Der Risikoindex (reduziert) wird für die originale Regel 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 Regel 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 Regelverletzungen, die für diese Regel zugelassen sind.

Detaillierte Informationen zum Thema

- *One Identity Manager Administrationshandbuch für Risikobewertungen*
- Risikomindernde Maßnahmen auf Seite 79

Verwandte Themen

- Erstellen von Regelbedingungen auf Seite 48
- Arbeitskopien für Complianceregeln erstellen auf Seite 46

Erweiterte Angaben für Complianceregeln

Auf dem Tabreiter **Erweitert** erfassen Sie zusätzliche Anmerkungen zur Regel sowie die Revisionsdaten.

Tabelle 15: Erweiterte Stammdaten einer Regel

Eigenschaft	Beschreibung
Regelnummer	Zusätzliche Bezeichnung der Regel.
Anmerkungen zur Implementierung	Freitextfeld für zusätzliche Erläuterungen. Die Anmerkungen zur Implementierung können beispielsweise inhaltliche Erläuterungen zur Regelbedingung umfassen.

Eigenschaft	Beschreibung
Zeitplan der Prüfung	Zeitplan, durch den die regelmäßige Überprüfung der Regel gestartet wird. Standardmäßig ist der Zeitplan **Berechnung der Complianceregeln** zugeordnet. Sie können einen eigenen Zeitplan zuordnen.
Zeitplan der Befüllung	Zeitplan, durch den die Neuberechnung der Hilfstabellen für die Regelprüfung gestartet wird. Standardmäßig ist der Zeitplan **Befüllung der Complianceregel Objekte** zugeordnet. Sie können einen eigenen Zeitplan zuordnen.
Status	Status der Regel bezüglich ihres Revisionsstandes.
Revisor	Person, die die Revision der Regel zuletzt vorgenommen hat.
Revisionsdatum	Datum der letzten Revision der Regel.
Revisionsbemerkung	Bemerkungen zur Revision, beispielsweise Ergebnisse, die für die nächste Revision wichtig sind.

Verwandte Themen

- Prüfen von Complianceregeln auf Seite 60
- Ermitteln potenzieller Regelverletzungen auf Seite 71

Regelvergleich

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

Tabelle 16: Ergebnis des Regelvergleichs

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

TIPP: Im Manager werden in der Kategorie **Identity Audit > Regeln > Arbeitskopien von Regeln > Geänderte Arbeitskopien** alle Arbeitskopien angezeigt, deren Bedingung nicht identisch ist mit der Bedingung der originalen Regel.

Detaillierte Informationen zum Thema

- Arbeitskopie und Original einer Regel vergleichen auf Seite 43

IT Shop Eigenschaften für Complianceregeln

In die Entscheidungsworkflows im IT Shop können Sie die Prüfung der Bestellungen auf Regelkonformität integrieren. Auf dem Tabreiter **IT Shop Eigenschaften** legen Sie fest, wie die Verletzungen einer Regel innerhalb eines Genehmigungsverfahrens für IT Shop Bestellungen behandelt werden.

HINWEIS: Dieser Tabreiter wird nur angezeigt, wenn die Regelbedingung in der vereinfachten Definition erstellt ist. Weitere Informationen finden Sie unter Erstellen von Regelbedingungen auf Seite 48.

Um IT Shop Eigenschaften für eine Regel zu erfassen

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ComplianceCheck | EnableITSettingsForRule**.
2. Aktivieren Sie im Manager auf dem Stammdatenformular der Regel, auf dem Tabreiter **Allgemein** die Option **Regel für zyklische Prüfung und Risikobewertung im IT Shop**.
3. Wählen Sie den Tabreiter **IT Shop Eigenschaften**.
4. Bearbeiten Sie die Stammdaten.
5. Speichern Sie die Änderungen.

Tabelle 17: IT Shop Eigenschaften

Eigenschaft	Beschreibung
Erkennung einer Regelverletzung	Gibt an, welche Regelverletzungen protokolliert werden. **Tabelle 18: Zulässige Werte** **Wert** / **Beschreibung** Neue Regelverletzung durch die Bestellung: Es werden nur Regelverletzungen protokolliert, die durch die Genehmigung der aktuellen Bestellung neu hinzukommen würden. Nicht genehmigte Ausnahmen: Es werden Regelverletzungen protokolliert, die durch die Genehmigung der aktuellen Bestellung neu hinzukommen würden. Zusätzlich werden auch bereits bekannte

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td></td><td>
<table>
<tr><th>Wert</th><th>Beschreibung</th></tr>
<tr><td></td><td>Regelverletzungen protokolliert, für die noch keine genehmigten Ausnahmen vorliegen.</td></tr>
<tr><td>Jede Verletzung der Compliance</td><td>Es werden alle Regelverletzungen protokolliert, unabhängig davon ob bereits eine Ausnahmegenehmigung vorliegt oder nicht.
Dieser Wert wird automatisch gesetzt, wenn die Option Explizite Ausnahmegenehmigung aktiviert wird.</td></tr>
</table>
</td></tr>
<tr><td>Explizite Ausnahmegenehmigung</td><td>Angabe, ob erneute Regelverletzungen einem Ausnahmegenehmiger vorgelegt werden oder ob bereits vorhandene Ausnahmegenehmigungen nachgenutzt werden sollen.
Tabelle 19: Zulässige Werte
<table>
<tr><th>Option ist</th><th>Beschreibung</th></tr>
<tr><td>aktiviert</td><td>Eine erkannte Regelverletzung wird immer zur Ausnahmegenehmigung vorgelegt, auch wenn es bereits eine genehmigte Ausnahme aus einer früheren Verletzung der Regel gibt.</td></tr>
<tr><td>deaktiviert</td><td>Eine erkannte Regelverletzung wird nicht erneut zur Ausnahmegenehmigung vorgelegt, wenn es bereits eine genehmigte Ausnahme aus einer früheren Verletzung der Regel gibt. Diese Ausnahmegenehmigung wird nachgenutzt und für die erkannte Regelverletzung automatisch eine Ausnahme zugelassen.</td></tr>
</table>
</td></tr>
</table>

Zusätzliche Aufgaben für Arbeitskopien

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

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 **Identity Audit > Regeln > Arbeitskopien von Regeln**.
2. Wählen Sie in der Ergebnisliste die Regel.
3. Wählen Sie die Aufgabe **Überblick über die Regel**.

Compliance Framework zuweisen

Über diese Aufgabe legen Sie fest, welche Compliance Frameworks für die ausgewählte Regel relevant sind. Compliance Frameworks dienen zur Einstufung von Attestierungsrichtlinien, Complianceregeln und Unternehmensrichtlinien entsprechend regulatorischer Anforderungen, wie beispielsweise interner Anforderungen oder Anforderungen laut Wirtschaftsprüfung.

Um Compliance Frameworks an eine Regel zuzuweisen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln > Arbeitskopien von Regeln**.
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

Risikomindernde Maßnahmen beschreiben Maßnahmen, die umgesetzt werden sollen, wenn eine Complianceregel verletzt wurde. Nach Umsetzung der Maßnahmen sollte die nächste Regelprüfung keine Regelverletzung ermitteln.

Um risikomindernde Maßnahmen zu bearbeiten

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

  HINWEIS: 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*.

Detaillierte Informationen zum Thema

- Risikomindernde Maßnahmen auf Seite 79
- Risikomindernde Maßnahmen zuweisen auf Seite 41
- Risikomindernde Maßnahmen erstellen auf Seite 42

Risikomindernde Maßnahmen zuweisen

Legen Sie fest, welche risikomindernden Maßnahmen für die ausgewählte Regel gelten.

Um risikomindernde Maßnahmen an eine Regel zuzuweisen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln > Arbeitskopien von Regeln**.
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.

HINWEIS: In Regeln über SAP Funktionen werden automatisch die risikomindernden Maßnahmen übernommen, die den zu prüfenden SAP Funktionen zugewiesen sind.

Voraussetzungen

- Der aktiven Regel sind ein Unternehmensbereich und eine Abteilung zugewiesen.
- Den zu prüfenden SAP Funktionen sind derselbe Unternehmensbereich und den zugehörigen Variablensets dieselbe Abteilung zugewiesen.

Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das SAP R/3 Compliance Add-on*.

Risikomindernde Maßnahmen erstellen

Um eine risikomindernde Maßnahme für Regeln zu erstellen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln > Arbeitskopien von Regeln**.
2. Wählen Sie in der Ergebnisliste eine Arbeitskopie.
3. Wählen Sie die Aufgabe **Risikomindernde Maßnahmen zuweisen**.
4. Wählen Sie die Aufgabe **Risikomindernde Maßnahme erstellen**.
5. Erfassen Sie die Stammdaten der risikomindernden Maßnahme.
6. Speichern Sie die Änderungen.
7. Wählen Sie die Aufgabe **Regeln zuweisen**.
8. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die Regeln, die zugewiesen werden sollen.
9. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Risikomindernde Maßnahmen auf Seite 79

Arbeitskopie aktivieren

Mit der Aktivierung der Arbeitskopie werden Änderungen auf die originale Regel übertragen. Zu einer neuen Arbeitskopie wird eine Regel angelegt. Nur originale Regeln werden in der Regelprüfung berücksichtigt.

Um eine Arbeitskopie zu aktivieren

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

TIPP: Im Manager werden in der Kategorie **Identity Audit > Regeln > Arbeitskopien von Regeln > Geänderte Arbeitskopien** alle Arbeitskopien angezeigt, deren Bedingung nicht identisch ist mit der Bedingung der originalen Regel.

Neu berechnen

An einer Arbeitskopie stehen verschiedene Aufgaben zur sofortigen Regelprüfung zur Verfügung. Weitere Informationen finden Sie unter Prüfen von Complianceregeln auf Seite 60.

Regel kopieren

Regeln können kopiert werden, um beispielsweise komplexe Regelbedingungen nachzunutzen. Es können sowohl die Arbeitskopien als auch die aktiven Regeln als Kopiervorlage genutzt werden.

Um eine Arbeitskopie zu kopieren

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln > Arbeitskopien von Regeln**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Regel 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 Regel vergleichen

Wenn Sie die Regelbedingung in einer Arbeitskopie geändert haben, können Sie die Auswirkungen dieser Änderung über einen Vergleich mit der originalen Regel ermitteln. Regeln lassen sich nur vergleichen, wenn zu einer Arbeitskopie eine originale Regel vorhanden ist. Das Ergebnis des Regelvergleichs wird auf dem Tabreiter **Regelvergleich** des Stammdatenformulars der Arbeitskopie dargestellt.

Um eine Regel mit der Arbeitskopie zu vergleichen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln > Arbeitskopien von Regeln**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Regelvergleich**.

Tabelle 20: Ergebnis des Regelvergleichs

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

Um den Regelvergleich als Bericht anzuzeigen

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

Verwandte Themen

- Regelvergleich auf Seite 37

Ausnahmegenehmiger pflegen

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

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

Um Personen als Ausnahmegenehmiger zu berechtigen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln > Arbeitskopien von Regeln**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Ausnahmegenehmiger pflegen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Allgemeine Stammdaten für Complianceregeln auf Seite 32
- Ausnahmegenehmiger auf Seite 28

Regelverantwortliche pflegen

Über diese Aufgabe können Sie die Regelverantwortlichen für die ausgewählte Regel pflegen. Personen können der auf dem Stammdatenformular eingetragenen Anwendungsrolle für Regelverantwortliche zugewiesen und aus der Anwendungsrolle entfernt werden.

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

Um Personen als Regelverantwortliche zu berechtigen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln > Arbeitskopien von Regeln**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
3. Wählen Sie die Aufgabe **Regelverantwortliche pflegen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Allgemeine Stammdaten für Complianceregeln auf Seite 32
- Regelverantwortliche auf Seite 27

SQL Definition aktivieren

Unter bestimmten Voraussetzungen kann die Regelbedingung direkt als SQL-Abfrage formuliert werden. Weitere Informationen finden Sie unter Regelbedingung als SQL-Abfrage auf Seite 58.

Zusätzliche Aufgaben für Complianceregeln

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

Überblick über Complianceregeln anzeigen

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

Um einen Überblick über eine Regel zu erhalten

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln**.
2. Wählen Sie in der Ergebnisliste die Regel.
3. Wählen Sie die Aufgabe **Überblick über die Regel**.

Arbeitskopien für Complianceregeln erstellen

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

Um eine Arbeitskopie zu erstellen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln**.
2. Wählen Sie in der Ergebnisliste die Regel.
3. Wählen Sie die Aufgabe **Arbeitskopie erstellen**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

TIPP: Im Manager werden in der Kategorie **Identity Audit > Regeln > Arbeitskopien von Regeln > Geänderte Arbeitskopien** alle Arbeitskopien angezeigt, deren Bedingung nicht identisch ist mit der Bedingung der originalen Regel.

Complianceregeln aktivieren und deaktivieren

Damit Regelverletzungen für eine Regel ermittelt werden können, aktivieren Sie die Regel. Um Regeln von der Regelprüfung auszuschließen, können Sie die Regeln deaktivieren. Eventuell vorhandene Regelverletzungen werden dabei durch den DBQueue Prozessor entfernt. Die Arbeitskopie einer Regel ist immer deaktiviert.

Um eine Regel zu aktivieren

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln**.
2. Wählen Sie in der Ergebnisliste die Regel.
3. Wählen Sie die Aufgabe **Regel aktivieren**.

Um eine Regel zu deaktivieren

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln**.
2. Wählen Sie in der Ergebnisliste die Regel.
3. Wählen Sie die Aufgabe **Regel deaktivieren**.

Neu berechnen

An einer Regel stehen verschiedene Aufgaben zur sofortigen Regelprüfung zur Verfügung. Weitere Informationen finden Sie unter Prüfen von Complianceregeln auf Seite 60.

Complianceregeln kopieren

Regeln können kopiert werden, um beispielsweise komplexe Regelbedingungen nachzunutzen. Es können sowohl die Arbeitskopien als auch die aktiven Regeln als Kopiervorlage genutzt werden.

Um eine Regel zu kopieren

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln**.
2. Wählen Sie in der Ergebnisliste die Regel.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Regel 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**.

Ausnahmegenehmiger pflegen

Über diese Aufgabe können Sie die Ausnahmegenehmiger für die ausgewählte Regel pflegen. Dafür weisen Sie der auf dem Stammdatenformular eingetragenen Anwendungsrolle für Ausnahmegenehmiger die Personen zu, die berechtigt sind, Ausnahmen für diese Regel zu genehmigen.

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

Um Personen als Ausnahmegenehmiger zu berechtigen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln**.
2. Wählen Sie in der Ergebnisliste die Regel.
3. Wählen Sie die Aufgabe **Ausnahmegenehmiger pflegen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Person und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für Complianceregeln auf Seite 32
- Ausnahmegenehmiger auf Seite 28

Regelverantwortliche pflegen

Über diese Aufgabe können Sie die Regelverantwortlichen für die ausgewählte Regel pflegen. Dafür weisen Sie der auf dem Stammdatenformular eingetragenen Anwendungsrolle für Ausnahmegenehmiger die Personen zu, die berechtigt sind, diese Regel zu bearbeiten.

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

Um Personen als Regelverantwortliche zu berechtigen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln**.
2. Wählen Sie in der Ergebnisliste die Regel.
3. Wählen Sie die Aufgabe **Regelverantwortliche pflegen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Person und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für Complianceregeln auf Seite 32
- Regelverantwortliche auf Seite 27

Erstellen von Regelbedingungen

In der Regelbedingung stellen Sie die Berechtigungen zusammen, die zu einer Regelverletzung führen. In der Regelbedingung werden die betroffene Personengruppe und die betroffenen Berechtigungen separat eingeschränkt. Über die betroffene Personengruppe werden die Personen und Identitäten ermittelt, auf die die Regelbedingung

anzuwenden ist. Über die betroffenen Berechtigungen werden die Eigenschaften definiert, die für die betroffene Personengruppe zu einer Regelverletzung führen. Die Berechtigungen werden über die Objektbeziehungen der betroffenen Personen ermittelt (Tabelle `PersonHasObject`).

TIPP: Wenn der Konfigurationsparameter **QER | ComplianceCheck | SimpleMode | NonSimpleAllowed** aktiviert ist, können Regelbedingungen sowohl im erweiterten Modus als auch in der vereinfachten Definition erstellt werden.

Um die vereinfachte Definition zu nutzen

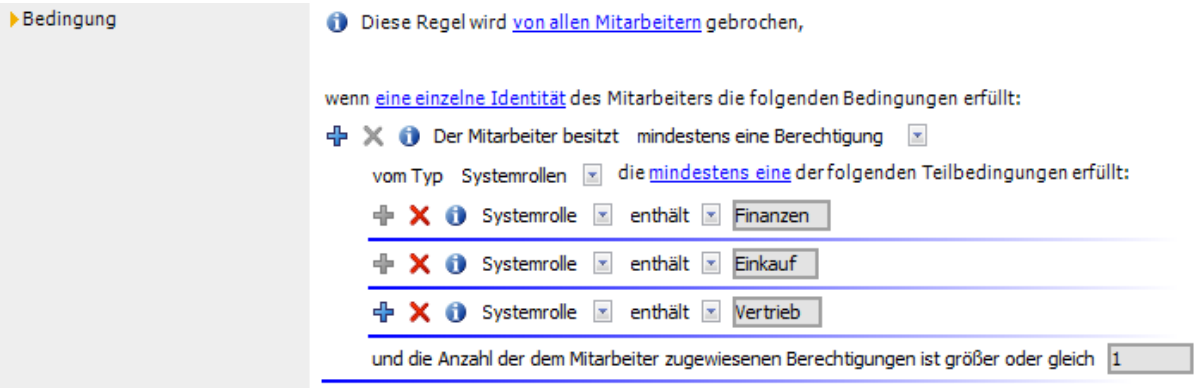
- Aktivieren Sie in den allgemeinen Stammdaten der Regel die Option **Regel für zyklische Prüfung und Risikobewertung im IT Shop**.

Weitere Informationen finden Sie unter Regelbedingungen im erweiterten Modus auf Seite 56.

Grundlagen zum Umgang mit dem Regeleditor

Bei der Formulierung der Regelbedingungen unterstützt Sie der Regeleditor. Hier können Sie vordefinierte Bedingungstypen und Operatoren nutzen. Die komplette Datenbankabfrage wird intern zusammengesetzt. Ist der Konfigurationsparamter **QER | ComplianceCheck | SimpleMode | ShowDescriptions** aktiviert, werden in der vereinfachten Definition zusätzliche Eingabefelder für eine nähere Beschreibung der einzelnen Regelblöcke angezeigt.

Abbildung 2: Regeleditor für die vereinfachte Definition von Regeln



Die Steuerelemente des Regeleditors stellen Operatoren und Eigenschaften zur Verfügung, die Sie zur Formulierung der Teilbedingungen benötigen. In einfachen Auswahllisten können Sie nur einen Eintrag auswählen. In erweiterten Auswahllisten mit einer hierarchischen Darstellung der Eigenschaften können Sie mehrere Einträge auswählen, die über eine Oder-Verknüpfung in die Bedingung eingebunden werden. Über Eingabefelder ist die freie Eingabe von Text zulässig. Die verfügbaren Auswahllisten und Eingabefelder werden dynamisch eingeblendet.

Eine Regelbedingung setzt sich aus mehreren Regelblöcken zusammen. Eine Regelverletzung wird festgestellt, wenn eine Person mit ihren Eigenschaften und Zuweisungen allen Regelblöcken zugeordnet werden kann.

Es gibt zwei Arten von Regelblöcken:

- Betroffene Personengruppe

  Jede Regel muss genau einen Regelblock enthalten, der die Personengruppe festlegt, auf welche die Regel angewendet werden soll. Standardmäßig werden alle Personen mit allen Identitäten beachtet. Sie können die Personengruppe jedoch weiter einschränken.

- Betroffene Berechtigungen

  Definieren Sie mindestens einen Regelblock, der die betroffenen Berechtigungen ermittelt. Hier werden die Eigenschaften zusammengestellt, die für die betroffene Personengruppe zu einer Regelverletzung führen. Folgende Berechtigungen können Sie in den Regelblöcken prüfen: Mitgliedschaften in hierarchischen Rollen, Systemberechtigungen, Systemrollen, Software, Ressourcen.

Mit dem Regeleditor können Sie beliebig viele Teilbedingungen innerhalb der einzelnen Regelblöcke einfügen und miteinander verknüpfen. Über die Optionen **Alle** und **Mindestens eine** legen Sie fest, ob eine oder alle Teilbedingungen eines Regelblocks erfüllt sein müssen.

Tabelle 21: Bedeutung der Symbole im Regeleditor

Symbol	Bedeutung
	Hinzufügen einer weiteren Teilbedingung beziehungsweise eines weiteren Regelblocks. Es wird eine neue Zeile für die Bedingungseingabe eingeblendet.
	Löschen der Teilbedingung beziehungsweise des Regelblocks. Die Zeile wird ausgeblendet.
	Öffnen des Vorschaufensters. Es werden die betroffenen Objekte angezeigt.
	Blendet die Liste der betroffenen Objekte im Vorschaufenster ein.

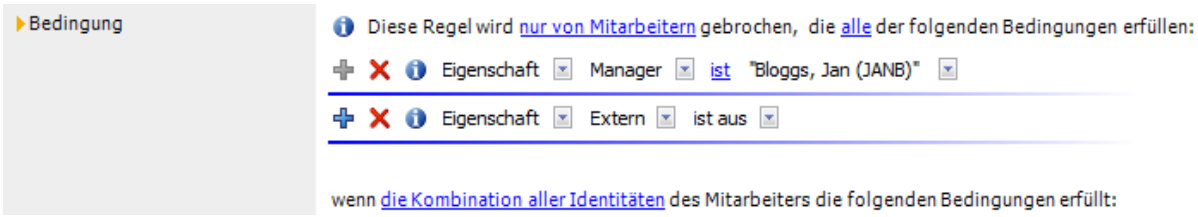
Um eine Vorschau der betroffenen Objekte anzuzeigen

1. Klicken Sie im Regeleditor an der Bedingung oder einer Teilbedingung .
2. Um die Liste der betroffenen Objekte anzuzeigen, klicken Sie im Vorschaufenster .

Festlegen der betroffenen Personengruppe

Jede Regeln muss genau einen Regelblock enthalten, der die Personengruppe festlegt.

Abbildung 3: Regelblock für die betroffene Personengruppe



Die betroffene Personengruppe grenzen Sie über folgende Optionen ein.

- Von allen Mitarbeitern

  Alle Personen werden berücksichtigt.

- Nur von Mitarbeitern, die alle/mindestens eine der folgenden Bedingungen erfüllen

  Die Personengruppe wird durch eine Bedingung eingeschränkt, beispielsweise "Alle Personen der Abteilung A" oder "Alle externen Personen". Um die betroffene Personengruppe zu ermitteln, formulieren Sie entsprechende Teilbedingungen.

  Für die Einschränkung der betroffenen Personengruppe legen Sie in der ersten Auswahlliste einer Teilbedingung den Bedingungstyp fest.

  Tabelle 22: Zulässige Bedingungstypen im Regeleditor

Bedingungstyp	Bedeutung
Eigenschaft	Eigenschaften der Personen. Die Auswahlliste der zulässigen Eigenschaften ist bereits auf die wichtigsten Eigenschaften einer Person eingeschränkt.
Für das Benutzerkonto mit dem Zielsystemtyp	Eigenschaften der Benutzerkonten der Personen mit dem gewählten Zielsystemtyp.
SQL Abfrage	Eingabe einer SQL Bedingung (Where-Klausel). Ausführliche Informationen zum Where-Klausel Assistenten finden Sie im *One Identity Manager Anwenderhandbuch für die Benutzeroberfläche der One Identity Manager-Werkzeuge*.

- Eine einzelne Identität

  Tabelle 23: Ergebnis der Regelprüfung

Die Regel ist ...	Bedingung
verletzt	Eine Subidentität oder die Hauptidentität einer Person erfüllt die Regelbedingung.
nicht verletzt	Die Hauptidentität erfüllt die Regelbedingung nur aufgrund ihrer Subidentitäten.

- Die Kombination aller Identitäten

  Die Regel ist verletzt, wenn

  - eine Subidentität oder die Hauptidentität einer Person die Regelbedingung erfüllt

    - ODER -

  - die Hauptidentität die Regelbedingung nur aufgrund ihrer Subidentitäten erfüllt.

Ausführliche Informationen zu Identitäten finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

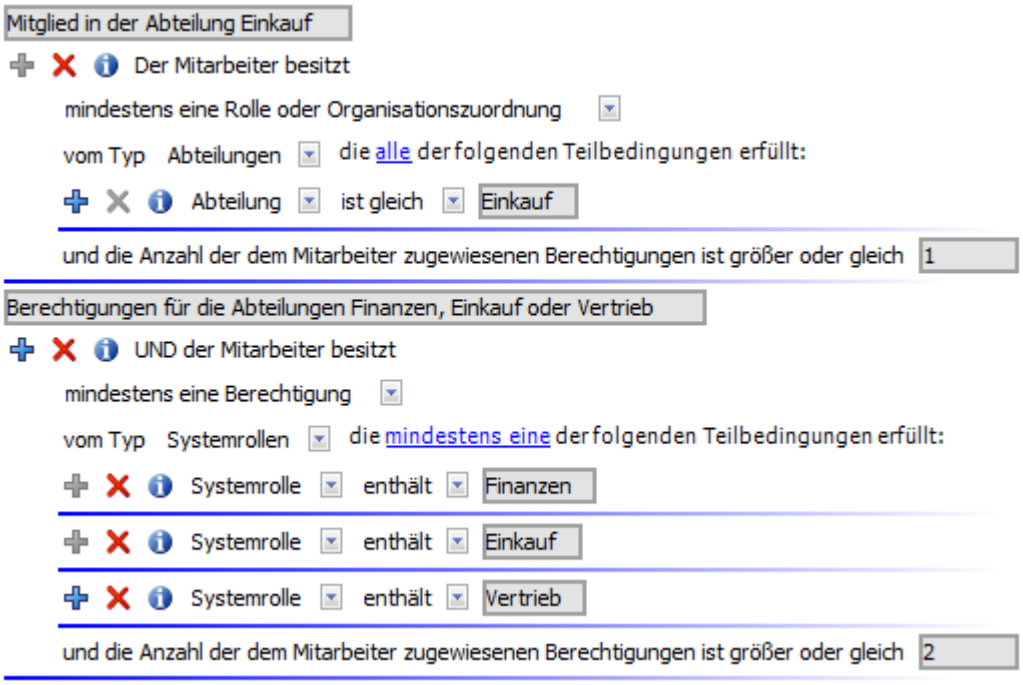
Verwandte Themen

- Beispiele für einfache Regeln auf Seite 54

Festlegen der betroffenen Berechtigungen

Um Zuweisungen in der Regel zu beachten, müssen Sie mindestens einen Regelblock definieren, der die betroffenen Berechtigungen für die Personengruppe ermittelt. Jeder Regelblock kann mehrere Teilbedingung enthalten. Die Teilbedingungen werden über die Optionen **alle** oder **mindestens eine** verknüpft.

Abbildung 4: Regelblock für die betroffenen Berechtigungen



Die betroffenen Berechtigungen grenzen Sie über folgende Optionen ein.

- Mindestens eine Berechtigung

  Pro Regelblock definieren Sie eine Berechtigung.

  Wählen Sie den Typ der Berechtigung, beispielsweise einen Zielsystemtyp oder den Typ **Ressourcen**, und definieren Sie die Teilbedingung (siehe Tabelle 24 auf Seite 53).

  Die Regeln können für alle im Unified Namespace abgebildeten Systemberechtigungen erstellt werden. Dabei wird in den Regelbedingungen auf die Datenbanksichten des Unified Namespace zugegriffen.

- Mindestens eine Rolle oder Organisationszuordnung

  Pro Regelblock definieren Sie die Mitgliedschaft in einer hierarchischen Rolle (Anwendungsrolle, Abteilung, Standort, Kostenstelle, Geschäftsrolle).

  Wählen Sie den Typ der Rolle, beispielsweise **Abteilungen**, und definieren Sie die Teilbedingung (siehe Tabelle 24 auf Seite 53).

- mindestens eine Funktion

  Geben Sie mindestens eine SAP Funktion an, durch welche die Regel verletzt wird.

  Diese Option kann nur ausgewählt werden, wenn das Modul Modul SAP R/3 Compliance Add-on vorhanden ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das SAP R/3 Compliance Add-on*.

- Anzahl der Berechtigungen

  Pro Regelblock legen Sie die Anzahl der Berechtigungen fest, die eine Person besitzen muss, damit die Regel verletzt ist.

  Standardmäßig wird eine Regelverletzung erkannt, wenn einer Person der betroffenen Personengruppe mindestens ein Objekt zugewiesen ist, das die Bedingung des Regelblocks erfüllt. Sie können diese Anzahl erhöhen. Der Wert **0** ist nicht zulässig.

Tabelle 24: Definieren der Teilbedingung

Teilbedingung	Beschreibung
Eigenschaften	Eigenschaften der Objekte, beispielsweise **Definierter Name** oder **Ressourcentyp**.
Zuordnungen in anderen Objekten	Zuordnungen der Objekte zu anderen Objekten, beispielsweise die Zuordnung einer Abteilung als primäre Abteilung verschiedener Personen.
Mitgliedschaften	Mitgliedschaften der Berechtigungen in hierarchischen Rollen und IT Shop-Strukturen. Zuweisungen zu Personen oder Arbeitsplätzen, wenn der Berechtigungstyp **Systemrollen** gewählt wurde. Zuweisungen von Unternehmensressourcen an die Rollen, wie beispielsweise `DepartmentHasADSGroup`.
Berechtigungselemente	Berechtigungselemente, die für das gewählte Zielsystem definiert sind. HINWEIS: Berechtigungselemente werden nur für kundendefinierte Zielsysteme erstellt.
Hat Zusatzeigenschaft	Zusatzeigenschaften, die den Objekten zugewiesen sind.
Hat Zusatzeigenschaft aus der Gruppe	Zusatzeigenschaften aus der gewählten Zusatzeigenschaftengruppe, die den Objekten zugewiesen sind.
Hat Zusatzeigenschaft mit Wertebereich	Zusatzeigenschaften, die den Objekten zugewiesen sind und für die ein Wertebereich festgelegt ist. In der Regel wird auf einen

Teilbedingung	Beschreibung
	konkreten Wert geprüft.
SQL Abfrage	Eingabe einer SQL Bedingung (Where-Klausel). Ausführliche Informationen zum Where-Klausel Assistenten finden Sie im *One Identity Manager Anwenderhandbuch für die Benutzeroberfläche der One Identity Manager-Werkzeuge*.

Verwandte Themen

- Beispiele für einfache Regeln auf Seite 54

Beispiele für einfache Regeln

Die folgenden Beispiele zeigen, wie Regeln mit Hilfe des Regeleditors erstellt werden und welche Auswirkungen die einzelnen Optionen haben.

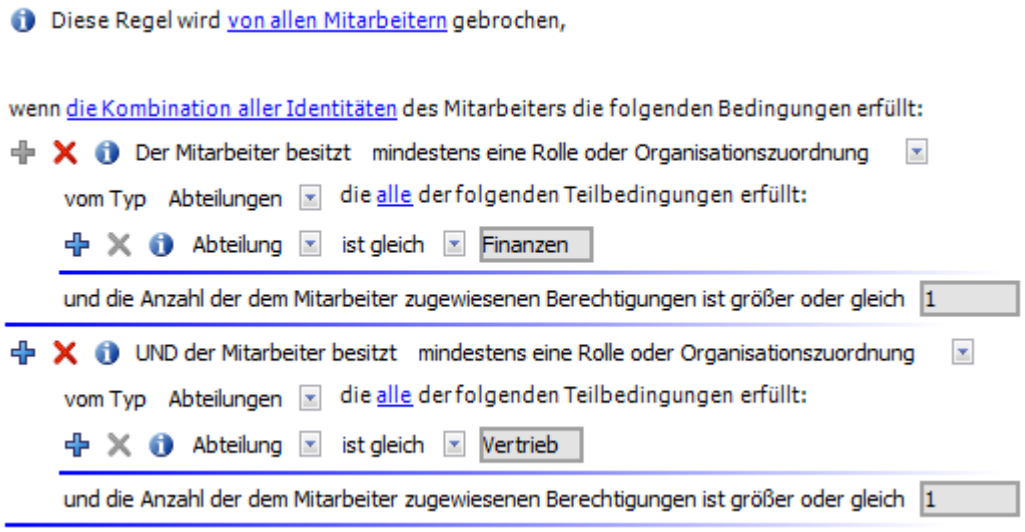
Beispiel 1

Personen der Abteilung A dürfen nicht gleichzeitig der Abteilung B angehören.

Definiert werden:

1. Die Option **von allen Mitarbeitern** und **die Kombination aller Identitäten** im Regelblock für die betroffene Personengruppe,
2. zwei Regelblöcke für die betroffenen Berechtigungen mit der Option **mindestens eine Rolle oder Organisationszuordnung**.

Abbildung 5: Regelbedingung für Beispiel 1



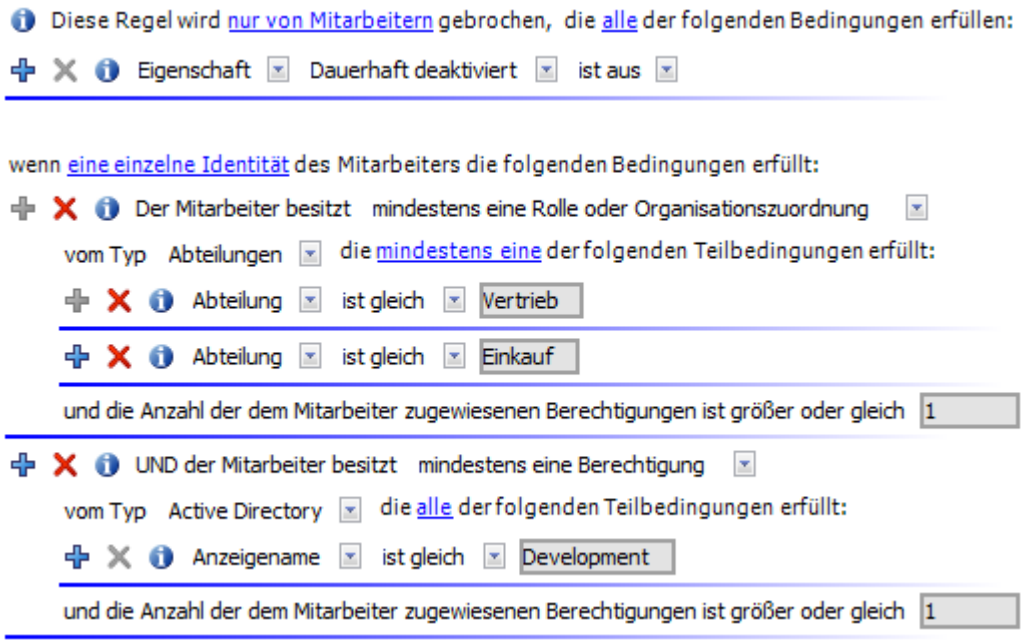
Beispiel 2

Personen, die der Abteilung Vertrieb oder der Abteilung Einkauf angehören, dürfen nicht auf die Active Directory Gruppe "Development" zugreifen. Diese Regel soll nur für Personen geprüft werden, die aktiviert sind.

Definiert werden:

1. die Optionen **nur von Mitarbeitern**, **alle** und **eine einzelne Identität** im Regelblock für die betroffene Personengruppe,
2. zwei Regelblöcke für die betroffenen Berechtigungen
    a. mit der Option **mindestens eine Rolle oder Organisationszuordnung** und
    b. mit der Option **mindestens eine Berechtigung**.

Abbildung 6: Regelbedingung für Beispiel 2



Beispiel 3

Alle zulässigen Berechtigungen werden über Systemrollen an die Personen zugewiesen. Eine Person darf maximal zwei Systemrolle besitzen. Wenn eine Person mehrere Identitäten besitzt, dann ist die Regel auch dann verletzt, wenn die Berechtigungen aller Subidentitäten zusammen zu einer Regelverletzung führen.

Es gibt drei Systemrollen: Paket für Abteilung Finanzen, Paket für Abteilung Einkauf, Paket für Abteilung Vertrieb

Jenny Basset hat zwei Subidentitäten. Der Hauptidentität und den beiden Subidentitäten sind jeweils eine Systemrolle zugewiesen.

Jenny Basset (HI): Paket für Abteilung Finanzen

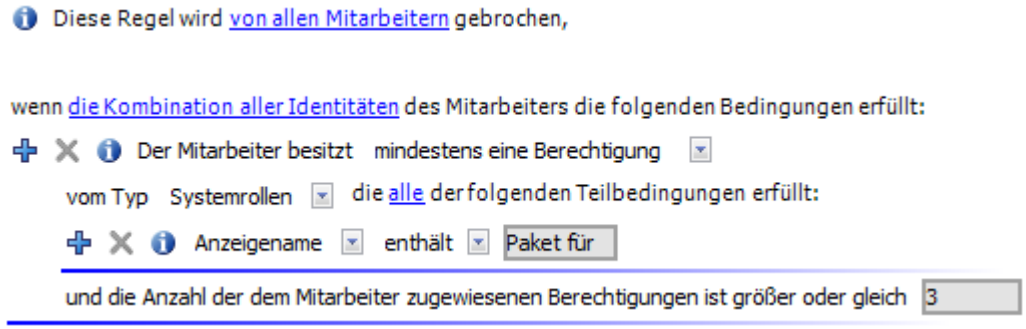
Jenny Basset (SI1): Paket für Abteilung Einkauf

Jenny Basset (SI2): Paket für Abteilung Vertrieb

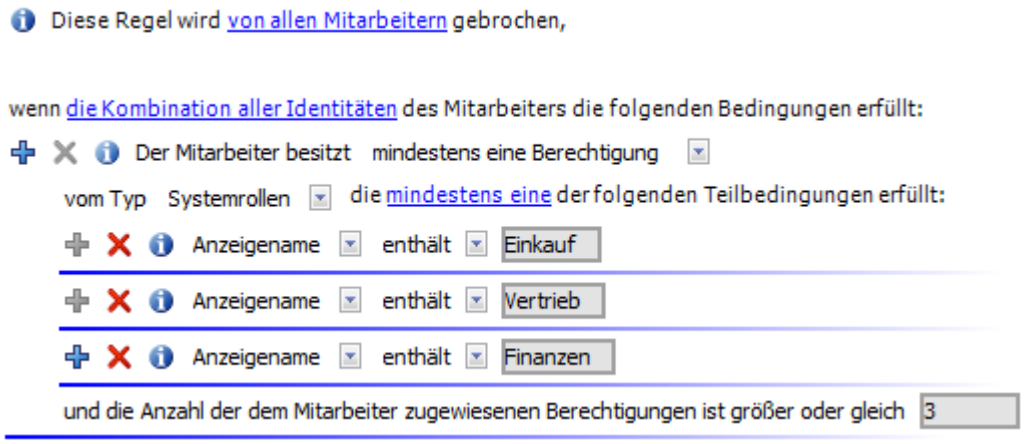
Definiert werden:

1. die Option **von allen Mitarbeitern** und **die Kombination aller Identitäten** im Regelblock für die betroffene Personengruppe
2. ein Regelblock für die betroffenen Berechtigungen mit der Option **mindestens eine Berechtigung** vom Typ **Systemrollen** die **alle** der folgenden Teilbedingungen erfüllt
3. eine Teilbedingung: **Anzeigename enthält** "Paket für"
4. Die Anzahl der dem Mitarbeiter zugewiesenen Berechtigungen ist größer oder gleich **3**.

Da die Hauptidentität von Jenny Basset aufgrund ihrer Subidentitäten alle drei Systemrollen besitzt, verletzt die Hauptidentität (und nur diese) die Regel.



Die Regelprüfung ermittelt das selbe Ergebnis, wenn die Regel folgendermaßen formuliert ist.



Regelbedingungen im erweiterten Modus

Es gibt zwei Möglichkeiten Regelbedingungen zu definieren, die vereinfachte Definition und den erweiterten Modus. Die vereinfachte Definition mit dem Regeleditor wird standardmäßig zum Erstellen von Regelbedingungen genutzt. Weitere Informationen finden Sie unter Grundlagen zum Umgang mit dem Regeleditor auf Seite 49.

Im erweiterten Modus werden in der Regelbedingung die Eigenschaften von Personen definiert, die zu einer Regelverletzung führen. Die Zuweisungen werden direkt über die jeweiligen Tabellen ermittelt, in denen die ausgewählten Objekte abgebildet sind (beispielsweise PersonHasSAPGroup oder Person).

Um den erweiterten Modus zu nutzen

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ComplianceCheck | SimpleMode | NonSimpleAllowed**.

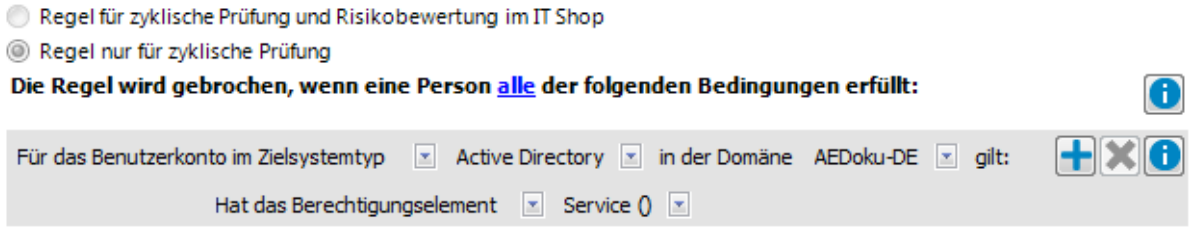
   Auf dem Stammdatenformular einer Regel werden zusätzlich die Optionen **Regel für zyklische Prüfung und Risikobewertung im IT Shop** und **Regel nur für zyklische Prüfung** angezeigt.
2. Aktivieren Sie die Option **Regel nur für zyklische Prüfung**.
3. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Es wird der Filterdesigner angezeigt.

HINWEIS:

- Nach der Eingabe einer Regelbedingung im erweiterten Modus können Sie nicht mehr zur vereinfachten Definition wechseln!
- Regeln im erweiterten Modus werden bei Regelprüfungen innerhalb von Genehmigungsverfahren für IT Shop-Bestellungen nicht berücksichtigt. Für diese Regeln können keine IT Shop Eigenschaften festgelegt werden. Der Tabreiter **IT Shop Eigenschaften** wird auf dem Stammdatenformular dieser Regeln nicht angezeigt.

Abbildung 7: Bedingung im erweiterten Modus



Die Regelbedingungen im erweiterten Modus beziehen sich auf das Basisobjekt **Personen** (Tabelle Person). Die komplette Datenbankabfrage wird intern zusammengesetzt:

```
Select Firstname, Lastname from Person where <Regelbedingung> order by 1,2
```

HINWEIS: Wenn Sie im Filterdesigner den Bedingungstyp **Für das Konto mit dem Zielsystemtyp** oder **Für die Berechtigung mit dem Zielsystemtyp** wählen, können nur Spalten ausgewählt werden, die im Unified Namespace abgebildet sind und für die die Spalteneigenschaft **Anzeige im Filterdesigner** aktiviert ist.

Ausführliche Informationen zur Bedienung des Filterdesigners finden Sie im *One Identity Manager Anwenderhandbuch für die Benutzeroberfläche der One Identity Manager-Werkzeuge*.

Tabelle 25: Zulässige Bedingungstypen

Bedingungstyp	Bedeutung
Eigenschaft	Eigenschaften der Personenobjekte. Die Auswahlliste der zulässigen Eigenschaften ist bereits auf die wichtigsten Eigenschaften einer Person eingeschränkt.
Für das Konto mit dem Zielsystemtyp	Benutzerkonto der Person. Die zulässigen Benutzerkonto-Eigenschaften richten sich nach der Auswahl des Zielsystems.
Für die Berechtigung mit dem Zielsystemtyp	Zielsystemgruppe der Person. Die zulässigen Gruppeneigenschaften richten sich nach der Auswahl des Zielsystems.
SQL Abfrage	Freie Eingabe einer SQL-Bedingung (Where-Klausel). Um den Where-Klausel-Assistenten zu nutzen, klicken Sie 🔨.

Regelbedingung als SQL-Abfrage

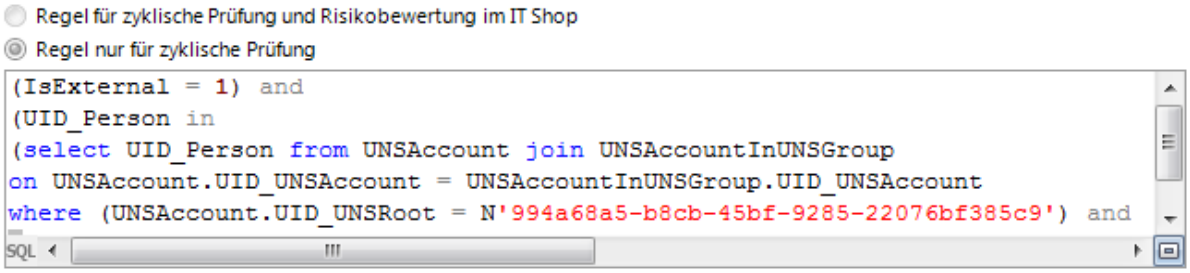
Regelbedingungen im erweiterten Modus können auch direkt als SQL-Abfrage formuliert werden.

Um eine Regelbedingung direkt als SQL-Abfrage zu formulieren

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ComplianceCheck | PlainSQL**.
2. Wählen Sie die Option **Regel nur für zyklische Prüfung**.
3. Wählen Sie die Aufgabe **SQL Definition aktivieren** an der Arbeitskopie.

HINWEIS: Wenn der Konfigurationsparameter **QER | ComplianceCheck | SimpleMode** deaktiviert ist und der Konfigurationsparameter **QER | ComplianceCheck | PlainSQL** aktiviert ist, können Regelbedingungen nur über eine SQL-Abfrage formuliert werden.

Abbildung 8: Direkte Eingabe der SQL-Abfrage



Complianceregeln löschen

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

Erstellen Sie vor dem Löschen einen Bericht über die Regel und ihre aktuellen Regelverletzungen, wenn Sie die Informationen (beispielsweise zur Revisionssicherheit) aufbewahren wollen.

Eine Regel kann gelöscht werden, wenn keine Regelverletzungen für die Regel vorhanden sind.

Um eine Regel zu löschen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln**.
2. Wählen Sie in der Ergebnisliste die zu löschende Regel.
3. Wählen Sie die Aufgabe **Regel deaktivieren**.

   Vorhandene Regelverletzungen werden durch den DBQueue Prozessor entfernt.
4. Klicken Sie in den Symbolleisten .

   Die Regel, das zugehörige Objekt für Regelverletzungen und die zugehörige Arbeitskopie werden gelöscht.

Regelprüfung

Zur Überprüfung einer Regel werden Verarbeitungsaufträge für den DBQueue Prozessor erzeugt. Der DBQueue Prozessor ermittelt für jede Regel, welche Personen die Regel verletzen. Durch Folgeaufträge werden Personen, die eine Regel verletzen, an das zugehörige Objekt für Regelverletzungen zugewiesen. Die für die Regeln festgelegten Ausnahmegenehmiger können die Regelverletzungen überprüfen und gegebenenfalls Ausnahmegenehmigungen erteilen.

Standardmäßig werden Berechtigungen, die eine Person erhält, weil sie ein administratives Benutzerkonto mit Gruppenidentität nutzen kann, bei der Regelprüfung berücksichtigt.

Um administrative Benutzerkonten mit Gruppenidentität von der Regelprüfung auszuschließen

- Deaktivieren Sie im Designer den Konfigurationsparameter **QER | ComplianceCheck | IncludeTSBPersonUsesAccount**.

  Objektbeziehungen aus der Tabelle `TSBPersonUsesAccount` werden bei der Berechnung der Einträge für die Tabelle `PersonHasObject` ignoriert.

Prüfen von Complianceregeln

Um aktuelle Regelverletzungen in der One Identity Manager-Datenbank zu ermitteln, kann die Regelprüfung über verschiedene Wege gestartet werden.

- Zeitgesteuerte Regelprüfung
- Automatische Regelprüfung nach Änderungen
- Ad-hoc-Regelprüfung

Bei der Regelprüfung werden nur die produktiven Regeln berücksichtigt. Deaktivierte Regeln werden nicht verarbeitet. Bei Verletzung einer Regel werden die betroffenen Personen dem entsprechenden Objekt für Regelverletzungen zugewiesen. Für diese Personen können Sie eine erneute Prüfung aller Regeln einstellen. Weitere Informationen finden Sie unter Auswertung der Regelprüfung auf Seite 62.

Zusätzlich zum Auffinden bestehender Regelverletzungen können mit dem One Identity Manager potenzielle Regelverletzungen von IT Shop Bestellungen und Geschäftsrollen erkannt werden. Weitere Informationen finden Sie unter Ermitteln potenzieller Regelverletzungen auf Seite 71.

Zeitgesteuerte Regelprüfung

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

Voraussetzungen

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

Detaillierte Informationen zum Thema

- Zeitpläne für die Regelprüfung auf Seite 13
- Complianceregeln aktivieren und deaktivieren auf Seite 46

Regelprüfung nach Änderungen

Beim Ändern und Löschen einer produktiven Regel wird der Verarbeitungsauftrag für die Regelprüfung sofort erzeugt. Alle Personen werden auf Erfüllung der betroffenen Regel geprüft.

Bei bestimmten Änderungen an den Berechtigungen können die Berechnungsaufträge zur Prüfung der Regeln sofort oder zyklisch eingestellt werden. Das gewünschte Verhalten

legen Sie über den Konfigurationsparameter **QER | ComplianceCheck | CalculateImmediately** fest. Wenn der Parameter aktiviert ist, wird der Verarbeitungsauftrag zur Neuberechnung von Regelverletzungen für eine Person sofort eingestellt. Ist der Parameter nicht aktiviert, wird der Verarbeitungsauftrag beim nächsten Lauf des zeitgesteuerten Auftrags eingestellt.

Um Regelprüfungen sofort nach relevanten Änderung zu veranlassen

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | ComplianceCheck | CalculateImmediately**.

  Der Verarbeitungsauftrag zur Neuberechnung von Regelverletzungen für eine Person wird bei relevanten Änderungen sofort eingestellt.

HINWEIS: Der Konfigurationsparameter wirkt nur bei relevanten Datenänderungen. Dazu gehören:

- Änderung der Personenstammdaten
- Änderung der Zuweisungen an Personen (beispielsweise Tabelle `PersonHasQERResource`)
- Änderung der Rollenmitgliedschaften von Personen
- Änderung der Mitgliedschaften in Systemberechtigungen (beispielsweise Tabelle `ADSAccountInADSGroup`)
- Änderung der Treffer einer SAP Funktion (Tabelle `SAPUserInSAPFunction`)

Ad-hoc-Regelprüfung

An einer Regel stehen verschiedene Aufgaben zur sofortigen Regelprüfung zur Verfügung.

Tabelle 26: Zusätzliche Aufgaben einer Regel

Aufgabe	Beschreibung
Regel neu berechnen	Alle Personen werden auf die Einhaltung der aktuellen Regel geprüft.
Neu berechnen für den angemeldeten Nutzer	Die angemeldete Person wird auf die Einhaltung aller Regeln geprüft.
Alles neu berechnen	Alle Personen werden auf die Einhaltung aller Regeln geprüft.

Beschleunigen der Regelprüfung

Die zeitgesteuerte Regelprüfung kann unter verschiedenen Bedingungen sehr lange laufen. Das kann beispielsweise der Fall sein, wenn zahlreiche Regeln existieren, in denen die betroffene Personengruppe nicht eingeschränkt ist ("Diese Regel wird von allen Mitarbeitern gebrochen"). Der One Identity Manager stellt zwei Konsistenzprüfungen

bereit, mit denen die Berechnung der betroffenen Personengruppen für eine Performanceverbesserung optimiert werden kann. Dabei wird die Datenmenge in der Hilfstabelle verringert.

Um die Regelprüfung zu optimieren, starten Sie diese Konsistenzprüfungen und reparieren Sie die ermittelten Regeln.

Um die Konsistenzprüfung auszuführen

1. Wählen Sie im Manager den Menüeintrag **Datenbank > Datenkonsistenz überprüfen**.
2. Klicken Sie in der Symbolleiste des Konsistenzeditors .
3. Klicken Sie in der Symbolleiste des Dialogfensters für die Testoptionen .
4. Aktivieren Sie die Tests **Content > Compliance > ComplianceRule change IsPersonStoreInverted to 1** und **Content > Compliance > ComplianceRule change IsPersonStoreInverted to 0**.
5. Klicken Sie **OK**.
6. Führen Sie die Konsistenzprüfung für das Objekt **Datenbank** durch.
7. Prüfen Sie die Analyseergebnisse.

   TIPP: Um Details zu einer Fehlermeldung zu erhalten

   1. Wählen Sie die Fehlermeldung.
   2. Klicken Sie in der Symbolleiste .
8. Um die Regelbedingung für eine betroffene Regel zu optimieren
   a. Wählen Sie die Fehlermeldung.
   b. Klicken Sie **Reparieren** sowohl für die originale Regel, als auch für die Arbeitskopie.

Ausführliche Informationen zu Konsistenzprüfungen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.

Verwandte Themen

- Arbeitskopien für Complianceregeln erstellen auf Seite 46

Auswertung der Regelprüfung

Jede Regel verweist auf ein eigenes Objekt für Regelverletzungen (Tabelle `NonCompliance`). Personen, die eine Regel verletzen, werden diesem Objekt zugewiesen (Tabelle `PersonInNonCompliance`). Zur Auswertung der Regelprüfung stehen zwei Formulare zur Verfügung, die folgende Fragen klären sollen:

- Welche Personen verletzen eine bestimmte Regel?
- Gegen welche Regeln verstößt eine bestimmte Person?

Welche Personen verletzen eine bestimmte Regel?

Um die Personen anzuzeigen, die eine Regel verletzen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regelverletzungen**.
2. Wählen Sie in der Ergebnisliste eine Regelverletzung.
3. Wählen Sie die Aufgabe **Regelverletzungen anzeigen**.

   Es werden alle Personen angezeigt, die dieser Regelverletzung zugewiesen sind.

Tabelle 27: Bedeutung der Symbole in der Auswertung für Regeln

Symbol	Bedeutung
	Personen, über deren Regelverletzung noch entschieden werden muss.
	Personen, für deren Regelverletzung eine Ausnahmegenehmigung erteilt wurde.
	Personen, für deren Regelverletzung keine Ausnahmegenehmigung erteilt wurde.

Gegen welche Regeln verstößt eine bestimmte Person?

Um die Regeln anzuzeigen, gegen die eine bestimmte Person verstößt

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste eine Person.
3. Wählen Sie den Bericht **Regelauswertung**.

   Hier werden zusätzlich zu den verletzten Regeln mit und ohne Ausnahmegenehmigung auch die Regeln dargestellt, gegen die die Person nicht verstößt.

Tabelle 28: Bedeutung der Symbole in der Regelauswertung für Personen

Symbol	Bedeutung
	Die Regel ist nicht verletzt.
	Die Regel ist verletzt. Für diese Regelverletzung wurde eine Ausnahmegenehmigung erteilt.
	Die Regel ist verletzt. Für diese Regelverletzung wurde keine Ausnahmegenehmigung erteilt.

Berichte über Regelverletzungen

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 Regeln, Regelgruppen und Compliance Frameworks können folgende Berichte erstellt werden.

HINWEIS: Abhängig von den vorhandenen Modulen können weitere Berichte zur Verfügung stehen.

Tabelle 29: Berichte über Regelverletzungen

Bericht	Beschreibung
Übersicht aller Zuweisungen (einer Regel)	Der Bericht zeigt alle Personen, die die ausgewählte Regel verletzen. Der Bericht stellt dar, in welchen Rollen einer Rollenklasse diese Personen Mitglied sind. Personen, die in keiner Rolle Mitglied sind, werden in diesem Bericht nicht berücksichtigt.
Überblick der Regelverletzungen (einer Regel)	Der Bericht stellt alle Regelverletzungen für die ausgewählte Regel zusammen. Es werden alle Personen mit den Objekten aufgelistet, die die Regel verletzen. Die Ergebnisliste ist gruppiert nach • Personen, über deren Regelverletzung noch entschieden werden muss, • Personen ohne Ausnahmegenehmigung, • Personen mit Ausnahmegenehmigung.
Historische Regelverletzungen anzeigen (einer Regel)	Der Bericht stellt alle historischen Regelverletzungen für die ausgewählte Regel zusammen. Es werden alle Personen aufgelistet, die die Regel verletzten, sowie der Zeitraum der Regelverletzung.
Überblick der Regelverletzungen (einer Regelgruppe)	Der Bericht stellt alle Regelverletzungen für die ausgewählte Regelgruppe zusammen. Es werden alle verletzten Regeln aufgelistet. Dazu wird die Anzahl der genehmigten, nicht genehmigten und nicht bearbeiteten Regelverletzungen angegeben.
Überblick der Regelverletzungen (eines Compliance Frameworks)	Der Bericht stellt alle Regelverletzungen für das ausgewählte Compliance Framework zusammen. Es werden alle verletzten Regeln aufgelistet. Dazu wird die Anzahl der genehmigten, nicht genehmigten und nicht bearbeiteten Regelverletzungen angegeben.
Detailauflistung der Regelverletzungen (eines Compliance Frameworks)	Der Bericht stellt alle Regelverletzungen für das ausgewählte Compliance Framework zusammen. Es werden alle verletzten Regeln aufgelistet. Zu jeder Regel sind die Personen angegeben, die die Regel verletzen, sowie Datum und Begründung der Entscheidung.

Verwandte Themen

- Übersicht aller Zuweisungen auf Seite 65

Übersicht aller Zuweisungen

Für einige Objekte, wie beispielsweise Berechtigungen, Complianceregeln oder Rollen wird der Bericht **Übersicht aller Zuweisungen** angezeigt. Der Bericht ermittelt alle Rollen, wie beispielsweise Abteilungen, Kostenstellen, Standorte, Geschäftsrollen und IT Shop Strukturen, in denen sich Personen befinden, die das gewählte Basisobjekt besitzen. Dabei werden sowohl direkte als auch indirekte Zuweisungen des Basisobjektes berücksichtigt.

Beispiele:

- Wird der Bericht für eine Ressource erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Ressource besitzen.
- Wird der Bericht für eine Gruppe oder andere Systemberechtigung erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Gruppe oder Systemberechtigung besitzen.
- Wird der Bericht für eine Complianceregel erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Complianceregel verletzen.
- Wird der Bericht für eine Abteilung erstellt, werden alle Rollen ermittelt, in denen die Personen der gewählten Abteilung ebenfalls Mitglied sind.
- Wird der Bericht für eine Geschäftsrolle erstellt, werden alle Rollen ermittelt, in denen die Personen der gewählten Geschäftsrolle ebenfalls Mitglied sind.

Um detaillierte Informationen über Zuweisungen anzuzeigen

- Um den Bericht anzuzeigen, wählen Sie in der Navigation oder in der Ergebnisliste das Basisobjekt und wählen Sie den Bericht **Übersicht aller Zuweisungen**.
- Wählen Sie über die Schaltfläche **Verwendet von** in der Symbolleiste des Berichtes die Rollenklasse, für die Sie ermitteln möchten, ob es Rollen gibt, in denen sich Personen mit dem ausgewählten Basisobjekt befinden.

  Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Personen befinden, denen das ausgewählte Basisobjekt zugewiesen ist. Die Bedeutung der Steuerelemente des Berichts ist in einer separaten Legende erläutert. Die Legende erreichen Sie über das Symbol in der Symbolleiste des Berichtes.
- Mit einem Maus-Doppelklick auf das Steuerelement einer Rolle zeigen Sie alle untergeordneten Rollen der ausgewählten Rolle an.

- Mit einem einfachen Mausklick auf die Schaltfläche im Steuerelement einer Rolle zeigen Sie alle Personen dieser Rolle an, die das Basisobjekt besitzen.
- Über den Pfeil rechts neben der Schaltfläche starten Sie einen Assistenten, mit dem Sie die Liste der angezeigten Personen zur Nachverfolgung speichern können. Dabei wird eine neue Geschäftsrolle erstellt und die Personen werden der Geschäftsrolle zugeordnet.

Abbildung 9: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 30: Bedeutung der Symbole in der Symbolleiste des Berichts

Symbol	Bedeutung
	Anzeigen der Legende mit der Bedeutung der Steuerelemente des Berichts.
	Speichern der aktuellen Ansicht des Berichts als Bild.
	Auswählen der Rollenklasse, über die der Bericht erstellt werden soll.
	Anzeige aller Rollen oder Anzeige der betroffenen Rolle.

Erteilen einer Ausnahmegenehmigung

Zuweisungen, die Regeln verletzen, können nachträglich genehmigt werden. Dafür können speziell berechtigte Personen Ausnahmegenehmigungen erteilen.

Voraussetzungen

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

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

Für Ausnahmegenehmiger muss geregelt werden, ob sie ihre eigenen Regelverletzungen genehmigen dürfen. Standardmäßig wird eine Person, die eine Regel verletzt, für diese Regel als Ausnahmegenehmiger ermittelt, wenn sie Mitglied der Anwendungsrolle **Ausnahmegenehmiger** für diese Regel ist. Damit kann sie sich eigene Regelverletzungen genehmigen.

Um zu verhindern, dass eine Person sich selbst eine Ausnahmegenehmigung erteilt

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | ComplianceCheck | DisableSelfExceptionGranting**.

  Personen, die eine Regel verletzen, werden nicht als Ausnahmegenehmiger für diese Regelverletzung ermittelt. Weder die Hauptidentität des Regelverletzers noch seine Subidentitäten können eine Ausnahmegenehmigung erteilen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Complianceregeln auf Seite 32
- *One Identity Manager Web Designer Web Portal Anwenderhandbuch*

Zeitliche Befristung von Ausnahmegenehmigungen

Ausnahmegenehmigungen können zeitlich befristet werden. Dafür kann an jeder Regel ein Gültigkeitszeitraum für Ausnahmegenehmigungen festgelegt werden. Nach Ablauf dieses Gültigkeitszeitraums werden geltende Ausnahmegenehmigungen automatisch annulliert. Ob eine Ausnahmegenehmigung weiterhin gültig ist, wird durch einen zeitgesteuerten Prozessauftrag überprüft.

Sobald eine Ausnahmegenehmigung erteilt wird, wird das Ablaufdatum aus dem aktuellen Datum und dem an der Regel hinterlegten Gültigkeitszeitraum berechnet. Eine Änderung des Gültigkeitszeitraums ist nur für künftige Ausnahmegenehmigungen wirksam. Das Ablaufdatum für bestehende Ausnahmegenehmigungen wird dadurch nicht verändert.

Um Ausnahmegenehmigungen zeitlich zu befristen

1. Erfassen Sie den Gültigkeitszeitraum für eine Regel.
   a. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln > Arbeitskopien von Regeln**.
   b. Wählen Sie in der Ergebnisliste die Arbeitskopie der Regel.
   c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
   d. Erfassen Sie auf dem Tabreiter **Allgemein**, im Eingabefeld **Max. Tage gültig** die Anzahl der Tage, die Ausnahmegenehmigungen für diese Regel gelten dürfen.

      Wenn der Wert **0** ist, sind die Ausnahmegenehmigungen unbefristet gültig.
   e. Speichern Sie die Änderungen.
   f. Um die Änderung auf die aktive Regel zu übertragen, wählen Sie die Aufgabe **Arbeitskopie aktivieren**.
2. Konfigurieren und aktivieren Sie im Designer den Zeitplan **Zurücksetzen von Ausnahmegenehmigungen für Complianceverletzungen**.

Ausführliche Informationen zum Einrichten von Zeitplänen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.

Ausnahmegenehmigungen im Manager erteilen

Um Regelverletzungen zu bearbeiten und Ausnahmegenehmigungen zu erteilen, nutzen Sie standardmäßig das Web Portal. Sie können Ausnahmegenehmigungen jedoch auch im Manager erteilen. Melden Sie sich dazu nicht-rollenbasiert am Manager an. Bei rollenbasierter Anmeldung steht diese Funktion im Manager nicht zur Verfügung.

Um Ausnahmegenehmigungen für alle Personen zu erteilen, die eine bestimmte Regel verletzen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regelverletzungen**.
2. Wählen Sie in der Ergebnisliste die Regelverletzung.
3. Wählen Sie die Aufgabe **Regelverletzungen anzeigen**.
4. Wählen Sie per Maus-Doppelklick die Person, der Sie eine Ausnahmegenehmigung erteilen möchten.

   Das Formular **Regelverletzung bearbeiten** wird geöffnet.
5. Um Detailinformationen über die Person zu erhalten, klicken Sie auf die Person.
6. Um Überblicksinformationen zur Regelverletzung zu erhalten, klicken Sie auf die Regelverletzung.
7. Erfassen Sie eine Begründung.
8. Um die Regelverletzung für diese Person zu genehmigen, klicken Sie **Ausnahme genehmigen**.

   Auf dem Formular werden die Eingabefelder **Entscheider** und **Entscheidung am** sowie die Optionen **Ausnahme ist genehmigt** und **Geprüft** ausgefüllt.
9. Um die Ausnahmegenehmigung für diese Person abzulehnen, klicken Sie **Ausnahme ablehnen**.

   Auf dem Formular werden die Eingabefelder **Entscheider** und **Entscheidung am** sowie die Option **Geprüft** ausgefüllt.
10. Speichern Sie die Änderungen.

Um Ausnahmegenehmigungen für alle Regeln zu erteilen, gegen die eine bestimmte Person verstößt

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie den Bericht **Regelauswertung**.
4. Wählen Sie per Maus-Doppelklick die Regelverletzung, für die Sie der Person eine Ausnahmegenehmigung erteilen möchten.

   Das Formular **Regelverletzung bearbeiten** wird geöffnet.

5. Um Detailinformationen über die Person zu erhalten, klicken Sie auf die Person.
6. Um Überblicksinformationen zur Regelverletzung zu erhalten, klicken Sie auf die Regelverletzung.
7. Erfassen Sie eine Begründung.
8. Um die Regelverletzung für diese Person zu genehmigen, klicken Sie **Ausnahme genehmigen**.

   Auf dem Formular werden die Eingabefelder **Entscheider** und **Entscheidung am** sowie die Optionen **Ausnahme ist genehmigt** und **Geprüft** ausgefüllt.
9. Um die Ausnahmegenehmigung für diese Person abzulehnen, klicken Sie **Ausnahme ablehnen**.

   Auf dem Formular werden die Eingabefelder **Entscheider** und **Entscheidung am** sowie die Option **Geprüft** ausgefüllt.
10. Speichern Sie die Änderungen.

Verwandte Themen

- Gegen welche Regeln verstößt eine bestimmte Person? auf Seite 63
- Welche Personen verletzen eine bestimmte Regel? auf Seite 63

Benachrichtigungen über Regelverletzungen

Im Anschluss an die Regelprüfung können E-Mail Benachrichtigungen über neue Regelverletzungen an die Ausnahmegenehmiger und Regelverantwortlichen 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 | ComplianceCheck | EmailNotification**.
3. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ComplianceCheck | 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

- Mailvorlagen für das Identity Audit bearbeiten auf Seite 76

Aufforderung zur Ausnahmegenehmigung

Wenn bei der Regelprüfung neue Regelverletzungen ermittelt werden, werden die Ausnahmegenehmiger benachrichtigt und zur Entscheidung aufgefordert.

Voraussetzungen

- Ausnahmegenehmigungen für Regelverletzungen sind zulässig.
- Der Regel ist eine Anwendungsrolle **Ausnahmegenehmiger** zugeordnet.
- Dieser Anwendungsrolle sind Personen zugewiesen.

Um Aufforderungen zur Ausnahmegenehmigung zu versenden

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

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

Verwandte Themen

- Complianceregeln erstellen und bearbeiten auf Seite 31
- Allgemeine Stammdaten für Complianceregeln auf Seite 32
- Maildefinitionen für das Identity Audit erstellen und bearbeiten auf Seite 73

Benachrichtigungen über Regelverletzungen ohne Ausnahmegenehmigung

Wenn bei der Regelprüfung neue Regelverletzungen ermittelt werden, für die keine Ausnahmegenehmigung erteilt werden kann, werden die Regelverantwortlichen benachrichtigt.

Voraussetzungen

- Ausnahmegenehmigungen für Regelverletzungen sind nicht zulässig.
- Der Regel ist eine Anwendungsrolle **Regelverantwortliche** zugeordnet.
- Dieser Anwendungsrolle sind Personen zugewiesen.

Um Regelverantwortliche über Regelverletzungen zu informieren

- Erfassen Sie an der Complianceregel die folgenden Daten.
  - **Ausnahmegenehmigung möglich**: deaktiviert
  - **Mailvorlage neue Verletzung**: Compliance - Unzulässige Regelverletzung aufgetreten

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

Verwandte Themen

- Complianceregeln erstellen und bearbeiten auf Seite 31
- Allgemeine Stammdaten für Complianceregeln auf Seite 32
- Maildefinitionen für das Identity Audit erstellen und bearbeiten auf Seite 73

Ermitteln potenzieller Regelverletzungen

Zusätzlich zum Auffinden bestehender Regelverletzungen können mit dem One Identity Manager potenzielle Regelverletzungen durch IT Shop Bestellungen erkannt werden. Dafür wird in die Genehmigungsverfahren im IT Shop ein Entscheidungsschritt mit dem Entscheidungsverfahren **CR - Regelprüfung (vereinfacht)** eingefügt.

Um potenzielle Regelverletzungen durch IT Shop Bestellungen zu erkennen, werden Hilfstabellen für die Objektzuordnungen und die betroffenen Personen ausgewertet. Diese Hilfstabellen werden regelmäßig durch den DBQueue Prozessor aktualisiert. Bei Änderungen an einer Regel werden die Hilfstabellen sofort neu berechnet.

Um andere Änderungen, wie beispielsweise die Änderung einer Berechtigung oder die Änderungen einer Zusatzeigenschaft in der Regelprüfung zu erfassen, ist in der One Identity Manager-Standardinstallation der Zeitplan **Befüllung der Complianceregel Objekte** enthalten. Dieser Zeitplan erzeugt zyklisch die Verarbeitungsaufträge zur

Aktualisierung der Hilfstabellen. Um den Zyklus für die Berechnung der Hilfstabellen an Ihre Erfordernisse anzupassen, erstellen Sie einen eigenen Zeitplan.

Um den Zyklus für die Berechnung der Hilfstabellen an Ihre Erfordernisse anzupassen

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Zeitpläne**.
2. Klicken Sie in der Ergebnisliste  .
3. Bearbeiten Sie die Stammdaten des Zeitplans.
4. Speichern Sie die Änderungen.
5. Wählen Sie die Aufgabe **Regeln (zur Befüllung) zuweisen** und weisen Sie den Zeitplan an alle Regeln zu, für die er gelten soll.
6. Speichern Sie die Änderungen.

HINWEIS:

Die Regelprüfung erreicht keine vollständige Überprüfung der Bestellungen. Unter folgenden Bedingungen ist es möglich, dass die Regelprüfung eine Regelverletzung nicht erkennt:

- Die Berechtigungen des Kunden ändern sich, nachdem die Hilfstabellen berechnet wurden.
- Bei der Bestellung von Mitgliedschaften in Geschäftsrollen oder Organisationen wird eine Regel durch ein Objekt verletzt, das über die bestellte Geschäftsrolle oder Organisation vererbt wird. Die Vererbung wird erst nach der Genehmigung der Bestellung berechnet und kann damit erst nach der nächsten Berechnung der Hilfstabellen erkannt werden.
- Der Kunde gehört erst durch die Bestellung zur betroffenen Personengruppe einer Regel.
- Die Regelbedingung wurde im erweiterten Modus oder als SQL-Abfrage erstellt.

TIPP: Eine vollständige Prüfung der Zuweisungen wird mit der zyklischen Prüfung der Complianceregeln über Zeitpläne erreicht. Damit werden alle Regelverletzungen erkannt, die durch die Bestellungen entstanden sind.

Unter folgenden Bedingungen ist es möglich, dass die Regelprüfung eine Regelverletzung erkennt, obwohl keine Regel verletzt wird:

- Zwei Produkte verletzen eine Regel, wenn sie gleichzeitig zugewiesen sind. Die Bestellungen dieser Produkte sind jedoch zeitlich begrenzt. Der Gültigkeitszeitraum überschneidet sich nicht. Dennoch wird eine potentielle Regelverletzung erkannt.

TIPP: Diese Bestellungen können nach Prüfung per Ausnahmegenehmigung genehmigt werden, sofern die Definition der verletzten Regel es zulässt.

Ausführliche Informationen zur Compliancеprüfung von IT Shop Bestellungen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Verwandte Themen

- Zeitpläne für die Regelprüfung auf Seite 13
- Complianceregeln an Zeitpläne zuweisen auf Seite 18

Mailvorlagen für Benachrichtigungen über das Identity Audit

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 **Identity Audit > Basisdaten zur Konfiguration > Mailvorlagen > Vordefiniert**.

Verwandte Themen

- Maildefinitionen für das Identity Audit erstellen und bearbeiten auf Seite 73
- Basisobjekte für Mailvorlagen über das Identity Audit auf Seite 74
- Verwenden von Hyperlinks zum Web Portal auf Seite 75
- Standardfunktionen für die Erstellung von Hyperlinks auf Seite 76
- Mailvorlagen für das Identity Audit bearbeiten auf Seite 76

Maildefinitionen für das Identity Audit 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.

Um eine neue Maildefinition zu erstellen

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

In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für das Identity Audit 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 **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. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > Mailvorlagen**.

   In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für das Identity Audit 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.

   HINWEIS: Wenn der **Common | MailNotification | DefaultCulture** aktiviert ist, wird beim Öffnen einer Mailvorlage die Maildefinition in der Standardsprache für E-Mail-Benachrichtigungen geladen und angezeigt.
3. Bearbeiten Sie die Betreffzeile und den Mailbody.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Basisobjekte für Mailvorlagen über das Identity Audit auf Seite 74
- Verwenden von Hyperlinks zum Web Portal auf Seite 75
- Standardfunktionen für die Erstellung von Hyperlinks auf Seite 76

Basisobjekte für Mailvorlagen über das Identity Audit

HINWEIS: Für Benachrichtigungen über Regelverletzungen verwenden Sie in den Mailvorlagen die Basisobjekte `ComplianceRule` oder `PersonInNonCompliance`.

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*.

Verwandte Themen

- Maildefinitionen für das Identity Audit erstellen und bearbeiten auf Seite 73
- Mailvorlagen für das Identity Audit bearbeiten auf Seite 76

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 im Identity Audit 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**.

Verwandte Themen

- Maildefinitionen für das Identity Audit erstellen und bearbeiten auf Seite 73
- Standardfunktionen für die Erstellung von Hyperlinks auf Seite 76

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:

```
$Script(VI_BuildComplianceLink_Show)$
```

Standardfunktionen für das Identity Audit

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

Tabelle 31: Funktionen des Skriptes VI_BuildComplianceLinks

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

Verwandte Themen

- Verwenden von Hyperlinks zum Web Portal auf Seite 75

Mailvorlagen für das Identity Audit 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 **Identity Audit > Basisdaten zur Konfiguration > Mailvorlagen**.

   In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für das Identity Audit 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 **Identity Audit > Basisdaten zur Konfiguration > Mailvorlagen**.

   In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für das Identity Audit 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 **Identity Audit > Basisdaten zur Konfiguration > Mailvorlagen**.

   In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für das Identity Audit 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 **Identity Audit > Basisdaten zur Konfiguration > Mailvorlagen**.

   In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für das Identity Audit genutzt werden können.
2. Wählen Sie in der Ergebnisliste die Mailvorlage.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Verwandte Themen

- Maildefinitionen für das Identity Audit erstellen und bearbeiten auf Seite 73

Risikomindernde Maßnahmen

Im Rahmen des Identity Audits werden die effektiven Berechtigungen von Personen, Rollen oder Benutzerkonten anhand regulatorischer Anforderungen überprüft. Für Unternehmen kann die Verletzung von regulatorischen Anforderungen unterschiedliche Risiken bergen. Um diese Risiken zu bewerten, können an Complianceregeln Risikoindizes angegeben werden. Diese Risikoindizes geben darüber Auskunft, wie riskant eine Verletzung der jeweiligen Regel 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 Complianceregel verletzt wurde. Nach Umsetzung der Maßnahmen sollte die nächste Regelprüfung keine Regelverletzung ermitteln.

Ein Beispiel für eine risikomindernde Maßnahme ist die Zuweisung von Systemberechtigungen nur über authorisierte Bestellungen im IT Shop. Wenn Systemberechtigungen über IT Shop Bestellungen an die Mitarbeiter vergeben werden, kann in das Genehmigungsverfahren der Bestellung eine Regelprüfung integriert werden. Systemberechtigungen, die zu einer Regelverletzung führen würden, werden damit nicht oder nur nach einer Ausnahmegenehmigung zugewiesen. Das Risiko, dass die Regeln verletzt werden, sinkt damit.

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*.

Risikomindernde Maßnahmen 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 32: 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.

Complianceregeln an risikomindernde Maßnahmen zuweisen

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

Um Complianceregeln 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 **Regeln zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Complianceregeln zu.

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

   Um eine Zuweisung zu entfernen

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

Überblick über risikomindernde Maßnahmen 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**.

Risikominderung berechnen

Die Signifikanzminderung einer risikomindernden Maßnahme gibt den Wert an, um den sich der Risikoindex einer Complianceregel 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.

Die Berechnung der Risikominderung für Regelverletzungen ist abhängig vom Konfigurationsparameter **QER | CalculateRiskIndex | MitigatingControlsPerViolation**.

Tabelle 33: Wirkung des Konfigurationsparameters auf die Berechnung der Risikominderung

Konfigurationsparameter	Wirkung
Deaktiviert	Es wird der reduzierte Risikoindex der Complianceregeln berechnet. Dabei werden alle risikomindernden Maßnahmen berücksichtigt, die einer Complianceregel zugewiesen sind.
Aktiviert	Der Risikoindex der Complianceregeln wird nicht reduziert. Damit entspricht der reduzierte Risikoindex dem erfassten Risikoindex der Complianceregeln. Es wird der reduzierte Risikoindex von Personen mit Regelverletzungen berechnet. Dabei werden alle risikomindernden Maßnahmen berücksichtigt, die bei einer Ausnahmegenehmigung an eine Regelverletzung zugewiesen wurden.

```
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 das Identity Audit

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

Tabelle 34: Übersicht der Konfigurationsparameter

Konfigurationsparameter	Bedeutung
QER | ComplianceCheck	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für das Identity Audit. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Sie die Modellbestandteile nutzen. 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*.
QER | ComplianceCheck | CalculateImmediately	Die Verarbeitungsaufträge für die Neuberechnung von Regelverletzungen werden bei relevanten Änderungen sofort eingestellt.
QER | ComplianceCheck | DisableSelfExceptionGranting	Ausschluss eines Regelverletzers aus dem Kreis der Ausnahmegenehmiger. Wenn der Konfigurationsparameter aktiviert ist, darf niemand seine eigene Regelverletzung genehmigen.
QER | ComplianceCheck | EmailNotification	Die Parameter zur Mailbenachrichtigung werden verwendet.

Konfigurationsparameter	Bedeutung
	Unterhalb des Parameters werden die Informationen zur Benachrichtigung während der Regelprüfung definiert.
QER | ComplianceCheck | EmailNotification | DefaultSenderAddress	Standard E-Mail-Adresse des Absenders zum Versenden von automatisch generierten Benachrichtigungen über Regelprüfungen. Ersetzen Sie den Standardwert durch eine gültige E-Mail-Adresse.
QER | ComplianceCheck | EnableITSettingsForRule	Die IT Shop Eigenschaften der Complianceregeln werden eingeblendet und können bearbeitet werden.
QER | ComplianceCheck | IncludeTSBPersonUsesAccount	Der Konfigurationsparameter legt fest, ob Nutzungsberechtigungen für Benutzerkonten mit Gruppenidentität bei der Regelprüfung berücksichtigt werden.
QER | ComplianceCheck | PlainSQL	Die Bearbeitung des SQL-Textes ist für Regeln im erweiterten Modus zulässig.
QER | ComplianceCheck | SimpleMode	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Definition von Regelbedingungen für die Complianceregeln. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Sie Regelbedingungen mit der vereinfachten Definition erstellen.
QER | ComplianceCheck | SimpleMode | NonSimpleAllowed	Regeln können im erweiterten Modus erstellt werden.
QER | ComplianceCheck | SimpleMode | ShowDescriptions	Im Regeleditor werden zusätzliche Eingabefelder für die Beschreibung der Complianceregeln angezeigt.
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. 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*.

Konfigurationsparameter	Bedeutung
QER | CalculateRiskIndex | MitigatingControlsPerViolation	Der Konfigurationsparameter regelt die Berechnung von Risikoindizes für Regelverletzungen. Ist der Parameter aktiviert, können Ausnahmegenehmiger risikomindernde Maßnahmen an Regelverletzungen zuweisen. Die Risikoindexberechnung berücksichtigt nur diese risikomindernden Maßnahmen. Ist der Parameter deaktiviert, berücksichtigt die Risikoindexberechnung die risikomindernden Maßnahmen, die an Complianceregeln zugewiesen sind.

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

Z