One Identity Manager 8.1.1

# Administrationshandbuch für Attestierungen

**Legende**

**WARNUNG: Das Symbol WARNUNG weist auf mögliche Personen- oder Sachschäden oder Schaden mit Todesfolge hin.**

**VORSICHT: Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.**

WICHTIG, HINWEIS, TIPP, MOBIL, or VIDEO: Ein Informationssymbol weist auf Begleitinformationen hin.

One Identity Manager Administrationshandbuch für Attestierungen
Aktualisiert - Juli 2019
Version - 8.1.1

# Inhalt

# 1

# Attestierung und Rezertifizierung

Mit der Attestierungsfunktion des One Identity Manager können Manager oder andere Complianceverantwortliche die Richtigkeit von Bearbeitungsrechten, Berechtigungen, Bestellungen oder Ausnahmegenehmigungen regelmäßig oder auf Anfrage bescheinigen. Die regelmäßige Bescheinigung von Berechtigungen wird im Allgemeinen als Rezertifizierung bezeichnet. Der One Identity Manager nutzt für Attestierungen und Rezertifizierungen die gleichen Abläufe.

Um Attestierungen durchführen zu können, werden im One Identity Manager Attestierungsrichtlinien definiert. Attestierungsrichtlinien legen fest, welche Objekte wann, wie oft und durch wen zu attestieren sind. Sobald eine Attestierung veranlasst wird, erstellt der One Identity Manager Attestierungsvorgänge, die alle notwendigen Informationen über die Attestierungsobjekte und die verantwortlichen Attestierer enthalten. Die verantwortlichen Attestierer prüfen die Attestierungsobjekte. Sie bestätigen korrekte Daten und veranlassen Änderungen, wenn Daten internen Regelungen widersprechen.

Attestierungsvorgänge zeichnen den gesamten Ablauf einer Attestierung auf. Im Attestierungsvorgang kann jeder einzelne Entscheidungsschritt der Attestierung revisionssicher nachvollzogen werden. Attestierungen werden regelmäßig durch zeitgesteuerte Aufträge ausgelöst. Bei Bedarf können einzelne Attestierungen auch manuell veranlasst werden.

Mit der Genehmigung oder Ablehnung eines Attestierungsvorgangs ist die Attestierung abgeschlossen. Wie mit abgelehnten oder genehmigten Attestierungen weiter verfahren werden soll, legen Sie unternehmensspezifisch fest.

TIPP: Der One Identity Manager stellt für verschiedene Datensituationen Standard-Attestierungsverfahren und Standard-Attestierungsrichtlinien bereit. Wenn Sie diese Standard-Attestierungsverfahren nutzen, können Sie konfigurieren, wie mit abgelehnten Attestierungen weiter verfahren werden soll.

Weitere Informationen finden Sie unter Standardattestierungen und der Entzug von Berechtigungen auf Seite 126.

***Um die Attestierungsfunktion zu nutzen***

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

# One Identity Manager Benutzer für die Attestierung

In die Attestierungen sind folgende Benutzer eingebunden.

**Tabelle 1: Benutzer**

| Benutzer | Aufgaben |
|---|---|
| Administratoren für Attestierungsvorgänge | Die Administratoren sind der Anwendungsrolle **Identity & Access Governance \| Attestierung \| Administratoren** zugewiesen.<br>Benutzer mit dieser Anwendungsrolle:<br>• Definieren Attestierungsverfahren und Attestierungsrichtlinien.<br>• Erstellen die Entscheidungsrichtlinien und Entscheidungsworkflows.<br>• Legen fest, nach welchen Entscheidungsverfahren die Attestierer ermittelt werden.<br>• Richten die Benachrichtigungen für Attestierungsvorgänge ein.<br>• Konfigurieren die Zeitpläne für die Attestierungen.<br>• Erfassen risikomindernde Maßnahmen.<br>• Erstellen und bearbeiten Risikoindex-Berechnungsvorschriften.<br>• Überwachen die Attestierungsvorgänge. |
| One Identity Manager Administratoren | • Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen.<br>• Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen.<br>• Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter.<br>• Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse.<br>• Erstellen und konfigurieren bei Bedarf Zeitpläne.<br>• Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien. |
| Attestierer | • Prüfen im Web Portal die Attestierungsobjekte. |

| Benutzer | Aufgaben |
| --- | --- |
| | • Bestätigen die Korrektheit der Daten.<br>• Veranlassen Änderungen, wenn Daten internen Regelungen widersprechen.<br><br>Die verantwortlichen Attestierer werden über die Entscheidungsverfahren ermittelt. |
| Compliance & Security Officer | Compliance & Security Officer müssen der Anwendungsrolle **Identity & Access Governance \| Compliance & Security Officer** zugewiesen sein.<br><br>Benutzer mit dieser Anwendungsrolle:<br><br>• Sehen im Web Portal alle Compliance-relevanten Informationen und deren Auswertungen. Dazu gehören Attestierungsrichtlinien, Unternehmensrichtlinien und Richtlinienverletzungen, Complianceregeln und Regelverletzungen sowie Risikoindex-Berechnungsvorschriften.<br>• Können Attestierungsrichtlinien bearbeiten. |
| Auditoren | Die Auditoren sind der Anwendungsrolle **Identity & Access Governance \| Auditoren** zugewiesen.<br><br>Benutzer mit dieser Anwendungsrolle:<br><br>• Sehen im Web Portal alle für ein Audit relevanten Daten. |
| Zentrale Entscheidergruppe | Die zentralen Entscheider müssen der Anwendungsrolle **Identity & Access Governance\| Attestierung \| Zentrale Entscheidergruppe** zugewiesen sein.<br><br>Benutzer mit dieser Anwendungsrolle:<br><br>• Entscheiden über Attestierungsvorgänge.<br>• Weisen Attestierungsvorgänge anderen Attestierern zu. |

# Basisdaten für Attestierungen

Die Rahmenbedingungen für Attestierungen und die zu attestierenden Objekte werden in Attestierungrichtlinien festgelegt. Um Attestierungsrichtlinien zu definieren, werden verschiedene Basisdaten benötigt.

| | |
| --- | --- |
| Attestierungstypen: | Attestierungstypen auf Seite 11 |
| Entscheidungsrichtlinien: | Entscheidungsrichtlinien für Attestierungen auf Seite 46 |
| Entscheidungsworkflows: | Entscheidungsworkflows für Attestierungen auf Seite 49 |

| | |
|---|---|
| Entscheidungsverfahren: | Entscheidungsverfahren einrichten auf Seite 80 |
| Attestierungsverfahren: | Attestierungsverfahren auf Seite 13 |
| Zeitpläne: | Zeitpläne auf Seite 19 |
| Compliance Frameworks: | Compliance Frameworks auf Seite 23 |
| Mailvorlagen: | Unternehmensspezifische Mailvorlagen für Benachrichtigungen auf Seite 38 |
| Zentrale Entscheidergruppe: | Zentrale Entscheidergruppe auf Seite 25 |
| Standardbegründungen: | Standardbegründungen für Attestierungen auf Seite 26 |

# Attestierungstypen

Attestierungstypen werden zur Gruppierung von Attestierungsverfahren genutzt. Sie erleichtern die Zuordnung eines passenden Attestierungsverfahrens zu Attestierungsrichtlinien.

***Um Attestierungstypen zu bearbeiten***

1. Wählen Sie die Kategorie **Attestierung | Basisdaten zur Konfiguration | Attestierungstypen**.
2. Wählen Sie in der Ergebnisliste einen Attestierungstyp und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   – ODER –

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

# Standard-Attestierungstypen

Standard-Attestierungstypen und ihre Zuweisungen zu Attestierungsverfahren können nicht bearbeitet werden.

Der One Identity Manager liefert standardmäßig Attestierungstypen aus. Diese Attestierungstypen sind den Standard-Attestierungsverfahren zugewiesen. Sie werden zum Einrichten von Attestierungsrichtlinien im Web Portal benötigt.

***Um Standard-Attestierungstypen anzuzeigen***

- Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Attestierungstypen | Vordefiniert**.

Ausführliche Informationen zur Verwendung der Standard-Attestierungstypen finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

# Zusätzliche Aufgaben für Attestierungstypen

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

## Überblick über den Attestierungstyp

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

***Um einen Überblick über einen Attestierungstyp zu erhalten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Attestierungstypen**.
2. Wählen Sie in der Ergebnisliste den Attestierungstyp.
3. Wählen Sie die Aufgabe **Überblick über den Attestierungstyp**.

## Attestierungsverfahren zuweisen

Über diese Aufgabe weisen Sie dem ausgewählten Attestierungstyp alle Attestierungsverfahren zu, die darunter zusammengefasst werden sollen.

***Um Attestierungsverfahren an einen Attestierungstyp zuzuweisen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Attestierungstypen**.
2. Wählen Sie in der Ergebnisliste den Attestierungstyp.
3. Wählen Sie die Aufgabe **Attestierungsverfahren zuweisen**.

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

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

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie das Attestierungsverfahren und doppelklicken Sie .
4. Speichern Sie die Änderungen.

# Attestierungsverfahren

Attestierungsverfahren legen das Basisobjekt der Attestierung fest. Sie definieren, welche Eigenschaften der Attestierungsobjekte zu attestieren sind. Die Informationen über die Attestierungsobjekte können als Bericht oder als Liste zur Verfügung gestellt werden.

***Um Attestierungsverfahren zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Attestierungsverfahren**.
2. Wählen Sie in der Ergebnisliste ein Attestierungsverfahren und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

# Allgemeine Stammdaten eines Attestierungsverfahrens

Für ein Attestierungsverfahren erfassen Sie folgende Eigenschaften.

**Tabelle 2: Allgemeine Stammdaten eines Attestierungsverfahrens**

| Eigenschaft | Beschreibung |
|---|---|
| Attestierungsverfahren | Beliebiger Name für das Attestierungsverfahren. |
| Attestierungstyp | Kriterium zur Gruppierung von Attestierungsverfahren. Attestierungstypen erleichtern die Zuordnung eines passenden Attestierungsverfahrens zu Attestierungsrichtlinien. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |
| Bericht | Bericht für die Attestierer mit allen notwendigen Informationen zu den Attestierungsobjekten.<br>In der Auswahlliste zu diesem Eingabefeld werden vordefinierte Berichte angeboten. Wenn Sie keinen Bericht zuordnen wollen, können Sie zusätzliche Informationen zu den Attestierungsobjekten in den Eingabefeldern **Eigenschaft 1-4 (Vorlage)** festlegen. |
| Tabelle | Datenbanktabelle, aus der die Attestierungsobjekte ermittelt werden (= Basisobjekt der Attestierung). Es werden alle Tabellen zur Auswahl angeboten, die folgende Bedingungen |

| Eigenschaft | Beschreibung |
|---|---|
| | erfüllen:<br>a. Die Tabelle enthält eine Spalte `XObjectKey`.<br>b. Der Tabellentyp ist **Tabelle**, **View**, **ReadOnly** oder **Proxy**.<br>c. Der Nutzungstyp ist **Nutzdaten**, **Materialisierte Daten** oder **Nur lesbare Daten**.<br>d. Es ist nicht die Tabelle `BaseTree`. Es ist keine mit `BaseTree` verbundene Zuordnungstabelle.<br>e. Die Tabelle gehört zum Anwendungsdatenmodell.<br>f. Die Tabelle ist nicht deaktiviert.<br>Ausführliche Informationen zu Tabellentypen und Nutzungstypen finden Sie im *One Identity Manager Konfigurationshandbuch*. |
| Präprozessorbedingung | Gibt an, von welchen präprozessorrelevanten Konfigurationsparametern das Attestierungsverfahren abhängig ist. Attestierungsverfahren, die durch eine Präprozessorbedingung deaktiviert sind, werden im One Identity Manager nicht angezeigt. |
| Gruppierungsspalte 1-3 (Vorlage) | Vorlage zur Bildung eines Wertes, nach dem die offenen Attestierungsvorgänge im Web Portal gruppiert und gefiltert werden können.<br>Geben Sie hier eine Bildungsregel in $-Notation an. Die Bildungsregel kann auf die Eigenschaften des Basisobjektes zugreifen und auf die Eigenschaften aller über Fremdschlüssel verbundenen Objekte. |
| Gruppierungsspalte 1-3 | Spaltenüberschriften für die Spalten **Gruppierungsspalte 1-3 (Vorlage)**. Die Spalten sind mehrsprachig. Um die Einträge zu übersetzen, klicken Sie . |
| Eigenschaft 1-4 (Vorlage) | Vorlage zur Bildung eines Wertes, der zusätzliche Informationen über das Attestierungsobjekt liefert. Mit diesen Feldern können zusätzliche Informationen zum Attestierungsobjekt im Web Portal angezeigt werden.<br>Geben Sie hier eine Bildungsregel in $-Notation an. Die Bildungsregel kann auf die Eigenschaften des Basisobjektes zugreifen und auf die Eigenschaften aller über Fremdschlüssel verbundenen Objekte. |
| Eigenschaft 1-4 | Spaltenüberschriften für die Spalten **Eigenschaft 1-4 (Vorlage)**. Die Spalten sind mehrsprachig. Um die Einträge zu übersetzen, klicken Sie . |

| Eigenschaft | Beschreibung |
|---|---|
| Risikoindex Vorlage | Vorlage zur Bildung eines Wertes für den Risikoindex des Attestierungsvorgangs.<br>Geben Sie hier eine Bildungsregel in $-Notation an. Die Bildungsregel kann auf die Eigenschaften des Basisobjektes zugreifen und auf die Eigenschaften aller über Fremdschlüssel verbundenen Objekte. |
| Objektbeziehung 1-3 (Vorlage) | Vorlage zur Bildung des Objektschlüssels eines Objekts, das in Beziehung zum Basisobjekt der Attestierung steht.<br>Geben Sie hier eine Bildungsregel in $-Notation an. Die Bildungsregel kann auf die Eigenschaften des Basisobjektes zugreifen und auf die Eigenschaften aller über Fremdschlüssel verbundenen Objekte.<br>Der gewünschte Anzeigewert dieses Objektes sollte in **Gruppierungsspalte 1-3 (Vorlage)** definiert werden. |

## Beispiel

Es sollen Active Directory Gruppenmitgliedschaften attestiert werden. Die Attestierungsvorgänge sollen nach dem Anzeigewert der Benutzerkonten, nach dem Anzeigewert der Active Directory Gruppen und nach dem Anzeigewert der verbundenen Person gruppiert werden können. Im Web Portal soll zu jeder Gruppenmitgliedschaft der kanonische Name der Active Directory Gruppe angezeigt werden. Der Risikoindex des Attestierungsvorgangs soll aus dem Risikoindex der Gruppenmitgliedschaft ermittelt werden. Der Objektschlüssel für die Objektbeziehung soll aus dem Active Directory Benutzerkonto ermittelt werden. Notwendige Informationen zu den Attestierungsobjekten sollen in einem Bericht zusammengefasst werden. Auf dem Stammdatenformular für das Attestierungsverfahren erfassen Sie dazu folgende Daten.

**Tabelle 3: Beispiel für die Definition eines Attestierungsvorgangs**

| Eigenschaft | Wert |
|---|---|
| Tabelle | Datenbanktabelle `ADSAccountInADSGroup` |
| Bericht | <Name des Reports> |
| Gruppierungsspalte 1 | $UID_ADSAccount[d]$ |
| Gruppierungsspalte 2 | $UID_ADSGroup[d]$ |
| Gruppierungsspalte 3 | $FK(UID_ADSAccount).UID_Person[d]$ |
| Eigenschaft 1 (Vorlage) | $FK(UID_ADSGroup).CanonicalName$ |
| Risikoindex Vorlage | $RiskIndexCalculated$ |
| Objektbeziehung 1 | $FK(UID_ADSAccount).XObjectKey$ |

### Detaillierte Informationen zum Thema

- Attestierungstypen auf Seite 11
- Berichte für Attestierungen definieren auf Seite 16

# Berichte für Attestierungen definieren

Berichte für die Attestierung definieren Sie mit dem Report Editor. Beachten Sie bei der Definition eines Berichts für Attestierungen Folgendes:

- Die Basistabelle für den Bericht muss identisch sein mit der Tabelle für das Attestierungsverfahren.
- Als Kategorie für den Bericht erfassen Sie **Attestation**. Dadurch wird der Bericht im Eingabefeld **Bericht** der Attestierungsverfahren zur Auswahl angeboten.
- Damit zu jedem Attestierungsobjekt ein Bericht mit den Informationen, die genau das Attestierungsobjekt betreffen, erstellt wird, definieren Sie im Bericht einen Parameter `ObjectKeyBase` für das Attestierungsobjekt. Nutzen Sie den Parameter in der Definition der Datenquelle für den Bericht im Feld **Bedingung**.

  Beispiel: `XObjectKey = @ObjectKeyBase`

### Standardberichte

Der One Identity Manager liefert einige Standardberichte für die Attestierung aus. Diese werden unter anderem in den Standard-Attestierungsverfahren genutzt. Standardberichte enthalten in ihrer Bezeichnung das Präfix **VI_**.

TIPP: Standardberichte können nicht geändert werden. Wenn Sie einen Standardbericht unternehmensspezifisch anpassen wollen, erstellen Sie eine Kopie des Berichts. Bearbeiten Sie die Kopie entsprechend ihren Erfordernissen und ordnen Sie die Kopie den Attestierungsverfahren zu.

# Standard-Attestierungsverfahren

Für die standardmäßige Attestierung neuer Benutzer sowie die Rezertifizierung aller in der One Identity Manager-Datenbank gespeicherten Personen stellt der One Identity Manager ein Standard-Attestierungsverfahren bereit. Darüber hinaus werden Standard-Attestierungsverfahren bereitgestellt, über die verschiedene Rollen, Benutzerkonten und im Unified Namespace abgebildete Systemberechtigungen attestiert werden können. Mit diesen Standard-Attestierungsverfahren können Sie auf einfachem Wege im Web Portal Attestierungsrichtlinien erstellen, um regulatorische Anforderungen zu erfüllen.

***Um Standard-Attestierungsverfahren anzuzeigen***

- Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Attestierungsverfahren | Vordefiniert**.

Ausführliche Informationen über die Nutzung von Standard-Attestierungsverfahren finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

### Verwandte Themen

- Attestierung und Rezertifizierung von Benutzern auf Seite 136
- Standardattestierungen und der Entzug von Berechtigungen auf Seite 126

# Zusätzliche Aufgaben für Attestierungsverfahren

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

## Überblick über das Attestierungsverfahren

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

***Um einen Überblick über ein Attestierungsverfahren zu erhalten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Attestierungsverfahren**.
2. Wählen Sie in der Ergebnisliste das Attestierungsverfahren.
3. Wählen Sie die Aufgabe **Überblick über das Attestierungsverfahren**.

## Entscheidungsrichtlinien zuweisen

Über diese Aufgabe weisen Sie dem ausgewählten Attestierungsverfahren die Entscheidungsrichtlinien zu, die mit diesem Attestierungsverfahren genutzt werden können. Es werden alle Entscheidungsrichtlinien angeboten, die für das Basisobjekt der Attestierung zugelassen sind.

***Um Entscheidungsrichtlinien an ein Attestierungsverfahren zuzuweisen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Attestierungsverfahren**.
2. Wählen Sie in der Ergebnisliste das Attestierungsverfahren.
3. Wählen Sie die Aufgabe **Entscheidungsrichtlinien zuweisen**.

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

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

***Um eine Zuweisung zu entfernen***

- Wählen Sie die Entscheidungsrichtlinie und doppelklicken Sie .

4. Speichern Sie die Änderungen.

Welche Entscheidungsrichtlinien zugelassen sind, ist abhängig von den Entscheidungsverfahren, die in den Entscheidungsrichtlinien verwendet werden. Für welche Tabellen ein Entscheidungsverfahren zugelassen ist, ist an den Entscheidungsverfahren festgelegt.

### Verwandte Themen

- Zulässige Entscheidungsverfahren für Tabellen festlegen auf Seite 85

## Kopie erstellen

Mit dieser Aufgabe können Sie eine Kopie des ausgewählten Attestierungsverfahrens erstellen. Kopien können Sie beispielsweise nutzen, um Standard-Attestierungsverfahren unternehmensspezifisch anzupassen.

***Um ein Attestierungsverfahren zu kopieren***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Attestierungsverfahren**.
2. Wählen Sie in der Ergebnisliste das Attestierungsverfahren.
3. Wählen Sie die Aufgabe **Kopie erstellen**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Entscheiden Sie, ob die Bedingungstypen für den Attestierungsassistenten im Web Portal ebenfalls kopiert werden sollen.

   Bedingungstypen werden benötigt, wenn Attestierungsrichtlinien mit dem Attestierungsassistenten im Web Portal erstellt oder bearbeitet werden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.
6. Bearbeiten Sie die Kopie des Attestierungsverfahrens und speichern Sie die Änderungen.

   Auf dem Stammdatenformular wird die Kopie des Attestierungsverfahrens mit der Bezeichnung **<Name des originalen Attestierungsverfahrens> (Kopie)** angezeigt. Sie können dieses Attestierungsverfahren umbenennen und bearbeiten.

# Zeitpläne

Mit Zeitplänen können Sie Attestierungen automatisieren. Sie legen fest, wann und wie häufig Attestierungsvorgänge erstellt werden sollen. Der One Identity Manager liefert einige Standardzeitpläne für die Attestierung aus.

***Um Zeitpläne zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Zeitpläne**.

   In der Ergebnisliste werden alle Zeitpläne angezeigt, die für Attestierungsrichtlinien (Tabelle `AttestationPolicy`) konfiguriert sind.
2. Wählen Sie in der Ergebnisliste einen Zeitplan aus und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Für einen Zeitplan erfassen Sie folgende Eigenschaften.

**Tabelle 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 . |
| Tabelle | Tabelle, für deren Daten der Zeitplan auswählbar ist. Zeitpläne für die Attestierung müssen auf die Tabelle `AttestationPolicy` verweisen. |
| Aktiviert | Angabe, ob der Zeitplan aktiv ist.<br>HINWEIS: Nur Zeitpläne, die aktiv sind, werden ausgeführt. |
| Zeitzone | Eindeutige Kennung der Zeitzone, nach dessen Zeitangaben der Zeitplan ausgeführt werden soll. Wählen Sie in der Auswahlliste zwischen **Universal Time Code** oder einer der Zeitzonen.<br>HINWEIS:<br>Wenn ein neuer Zeitplan angelegt wird, ist die Zeitzone des Clients vorausgewählt, von dem Sie den Manager gestartet haben. |

| Eigenschaft | Bedeutung |
|---|---|
| Beginn (Datum) | Tag, an dem der Zeitplan erstmalig ausgeführt werden soll. |
| Gültigkeitszeitraum | Zeitraum, innerhalb dessen der Zeitplan ausgeführt werden soll.<br>• Wenn der Zeitplan unbefristet ausgeführt werden soll, wählen Sie die Option **Unbegrenzte Laufzeit**.<br>• Um einen Gültigkeitszeitraum festzulegen, wählen Sie die Option **Begrenzte Laufzeit** und erfassen Sie im Eingabefeld **Ende (Datum)** den Tag, an dem der Zeitplan letztmalig ausgeführt werden soll. |
| Auftreten | Intervall, in welchem der Auftrag ausgeführt wird. Als Intervalltypen sind **minütlich**, **stündlich**, **täglich**, **wöchentlich**, **monatlich** und **jährlich** zulässig.<br>Für den Intervalltyp **wöchentlich** legen Sie den genauen Wochentag fest. Für den Intervalltyp **monatlich** legen Sie den Tag des Monats fest (1.-31. Tag eines Monats). Für den Intervalltyp **jährlich** legen Sie den Tag des Jahres fest (1. bis 366.Tag eines Jahres).<br>HINWEIS: Würde bei Intervalltyp **monatlich** mit der Angabe des Subintervalls **29**, **30** oder **31** die Ausführung des Zeitplans erst im Folgemonat erfolgen, so wird der letzte Tag des aktuellen Monats verwendet.<br>Beispiel:<br>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.<br>Zeitpläne mit dem Intervalltyp **jährlich** und dem Subintervall **366** werden nur in Schaltjahren ausgeführt. |
| Startzeit | Feste Startzeit für die Intervalltypen **täglich**, **wöchentlich**, **monatlich** und **jährlich**. Geben Sie die Uhrzeit in der Ortszeit der ausgewählten Zeitzone an.<br>Für die Intervalltypen **minütlich** und **stündlich** wird der Startzeitpunkt aus der Ausführungsfrequenz und dem Intervalltyp berechnet. |
| Wiederholen alle | Ausführungsfrequenz, mit welcher der zeitgesteuerte Auftrag innerhalb des gewählten Zeitintervalls ausgeführt werden soll. Für den Intervalltyp **wöchentlich** wählen Sie mindestens einen Wochentag. |
| Letzter geplanter Lauf/Nächster geplanter Lauf | Ausführungszeitpunkte, die durch den DBQueue Prozessor berechnet wurden. Die Ausführungszeitpunkte werden während der Ausführung eines Zeitplans neu ermittelt. Der Zeitpunkt der |

| Eigenschaft | Bedeutung |
|---|---|
| | nächsten Ausführung wird anhand des festgelegten Intervalls, der Ausführungsfrequenz und der Startzeit berechnet.<br>HINWEIS: Der One Identity Manager zeigt die Ausführungszeitpunkte in der Ortszeit der ausgewählten Zeitzone an. Sommerzeitumstellungen werden bei der Berechnung berücksichtigt. |

# Standardzeitpläne

Der One Identity Manager stellt standardmäßig folgende Zeitpläne für die Attestierung bereit.

**Tabelle 5: Standardzeitpläne für die Attestierung**

| Zeitplan | Beschreibung |
|---|---|
| Half-Yearly | Standardzeitpläne für beliebige Attestierungen. |
| Monthly | |
| Quarterly | |
| Weekly (Monday) | |
| Yearly | |
| Deactivated | Standardzeitplan für Standardattestierungsrichtlinien.<br>Der Zeitplan ist standardmäßig deaktiviert und sollte nicht aktiviert werden. Um Attestierungen durchzuführen, ordnen Sie den Attestierungsrichtlinien einen anderen Zeitplan zu und aktivieren Sie diesen. |
| Daily | Standardzeitplan für beliebige Attestierungen.<br>Der Zeitplan ist standardmäßig der Attestierungsrichtlinie **Zertifizierung neuer Benutzer** zugeordnet. |

## Verwandte Themen

- Rezertifizierung vorbereiten auf Seite 149
- Zeitgesteuerte Attestierungen auf Seite 146

# Zusätzliche Aufgaben für Zeitpläne

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

## Überblick zum Zeitplan

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

***Um einen Überblick über einen Zeitplan zu erhalten***

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

## Attestierungsrichtlinien zuweisen

Über diese Aufgabe weisen Sie dem ausgewählten Zeitplan die Attestierungsrichtlinien zu, die mit diesem Zeitplan ausgeführt werden sollen. Auf dem Zuordnungsformular werden alle Attestierungsrichtlinien angezeigt, denen der ausgewählte Zeitplan zugewiesen ist.

***Um Attestierungsrichtlinien an einen Zeitplan zuzuweisen***

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

***Um eine Zuordnung zu ändern***

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

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

   Dieser Attestierungsrichtlinie wird der aktuell ausgewählte Zeitplan zugeordnet.
6. Speichern Sie die Änderungen.

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

## Zeitplan sofort ausführen

HINWEIS: Wenn ein Zeitplan gestartet wird, werden Attestierungen für alle aktivierten Attestierungsrichtlinien, denen der Zeitplan zugeordnet ist, ausgeführt.

***Um einen Zeitplan sofort zu starten***

1. Wählen Sie im Manager die Kategorie **Attestierung | 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.

# Compliance Frameworks

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

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

***Um Compliance Frameworks zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Compliance Frameworks**.
2. Wählen Sie in der Ergebnisliste ein Compliance Framework und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

   Klicken Sie in der Ergebnisliste **Neu**.
3. Bearbeiten Sie die Stammdaten des Compliance Frameworks.
4. Speichern Sie die Änderungen.

Für Compliance Frameworks erfassen Sie folgende Eigenschaften.

**Tabelle 6: Eigenschaften eines Compliance Frameworks**

| Eigenschaft | Beschreibung |
|---|---|
| Compliance | Bezeichnung des Compliance Frameworks. |

| Eigenschaft | Beschreibung |
|---|---|
| Framework | |
| 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 Attestierungsrichtlinien bearbeiten dürfen, die diesem Compliance Framework zugeordnet sind. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |

# Zusätzliche Aufgaben für Compliance Frameworks

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

## Überblick über das Compliance Framework

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

***Um einen Überblick über ein Compliance Framework zu erhalten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Compliance Frameworks**.
2. Wählen Sie in der Ergebnisliste das Compliance Framework.
3. Wählen Sie die Aufgabe **Überblick über das Compliance Framework**.

## Attestierungsrichtlinien zuweisen

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

***Um Attestierungsrichtlinien an Compliance Frameworks zuzuweisen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Compliance Frameworks**.
2. Wählen Sie in der Ergebnisliste das Compliance Framework.
3. Wählen Sie die Aufgabe **Attestierungsrichtlinien zuweisen**.

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

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

***Um eine Zuweisung zu entfernen***

- Wählen Sie die Attestierungsrichtlinie und doppelklicken Sie ✓.

4. Speichern Sie die Änderungen.

# Zentrale Entscheidergruppe

Mitunter können Attestierungsvorgänge nicht entschieden werden, da ein Attestierer nicht verfügbar ist oder keinen Zugang zu den One Identity Manager Werkzeugen hat. Um solche Attestierungsvorgänge dennoch abzuschließen, können Sie eine zentrale Entscheidergruppe festlegen, deren Mitglieder berechtigt sind, zu jedem Zeitpunkt in die Genehmigungsverfahren einzugreifen.

Im One Identity Manager ist eine Standardanwendungsrolle für die zentrale Entscheidergruppe vorhanden. Weisen Sie dieser Anwendungsrolle alle Personen zu, die berechtigt sind in besonderen Fällen Attestierungen zu genehmigen, abzulehnen, abzubrechen oder andere Attestierer zu beauftragen. Ausführliche Informationen zu Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

**Tabelle 7: Standardanwendungsrolle für zentrale Entscheider**

| Benutzer | Aufgaben |
|---|---|
| Zentrale Entscheidergruppe | Die zentralen Entscheider müssen der Anwendungsrolle **Identity & Access Governance\| Attestierung \| Zentrale Entscheidergruppe** zugewiesen sein.<br>Benutzer mit dieser Anwendungsrolle:<br>• Entscheiden über Attestierungsvorgänge.<br>• Weisen Attestierungsvorgänge anderen Attestierern zu. |

***Um Mitglieder in die zentrale Entscheidergruppe aufzunehmen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Zentrale Entscheidergruppe**.
2. Wählen Sie die Aufgabe **Personen zuweisen**.

   Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu, die berechtigt

sind alle Attestierungen zu entscheiden.

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

***Um eine Zuweisung zu entfernen***

- Wählen Sie die Person und doppelklicken Sie .

3. Speichern Sie die Änderungen.

### Detaillierte Informationen zum Thema

- Attestierungen durch die zentrale Entscheidergruppe auf Seite 100

# Standardbegründungen für Attestierungen

Bei Attestierungen 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 Attestierer im Web Portal einen geeigneten Text auswählen und am Attestierungsvorgang hinterlegen.

Standardbegründungen werden in der Attestierungshistorie angezeigt.

***Um Standardbegründungen zu bearbeiten***

1. Wählen Sie die Kategorie **Attestierung | 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 8: Allgemeine Stammdaten einer Standardbegründung**

| Eigenschaft | Beschreibung |
|---|---|
| Standardbegründung | Begründungstext, so wie er im Web Portal und in der Attestierungshistorie angezeigt werden soll. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |
| Automatische Entscheidung | Angabe, ob der Begründungstext nur für automatischen Entscheidungen durch den One Identity Manager genutzt werden soll. Diese Standardbegründung kann bei manuellen |

| Eigenschaft | Beschreibung |
| --- | --- |
| | Entscheidungen im Web Portal nicht ausgewählt werden.<br>Damit die Standardbegründung im Web Portal ausgewählt werden kann, deaktivieren Sie die Option. |
| Zusätzlicher Text erforderlich | Angabe, ob bei der Attestierung eine zusätzliche Begründung als Freitext erfasst werden soll. |
| Nutzungstyp | Nutzungstyp der Standardbegründung. Um Standardbegründungen im Web Portal filtern zu können, ordnen Sie einen oder mehrere Nutzungstypen zu. |

## Vordefinierte Standardbegründungen

Der One Identity Manager stellt vordefinierte Standardbegründungen bereit. Diese Standardbegründungen werden bei automatischen Entscheidungen durch den One Identity Manager am Attestierungsvorgang eingetragen.

***Um vordefinierte Standardbegründungen anzuzeigen***

- Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten | Standardbegründungen | Vordefiniert**.

# Attestierungsrichtlinien

Attestierungsrichtlinien legen die konkreten Bedingungen für Attestierungen fest. Auf dem Stammdatenformular stellen Sie Attestierungsverfahren, Entscheidungsrichtlinie und Zeitplan für die Attestierung zusammen. Über eine Where-Klausel können Sie die Attestierungsobjekte einschränken.

***Um Attestierungsrichtlinien zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste eine Attestierungsrichtlinie und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

# Allgemeine Stammdaten von Attestierungsrichtlinien

Für Attestierungsrichtlinien erfassen Sie folgende Daten.

**Tabelle 9: Allgemeine Stammdaten einer Attestierungsrichtlinie**

| Eigenschaft | Beschreibung |
|---|---|
| Attestierungsrichtlinie | Bezeichnung der Attestierungsrichtlinie. |
| Attestierungsverfahren | Attestierungsverfahren, das für die Attestierung genutzt werden soll. Die Attestierungsverfahren werden in der Auswahlliste nach Attestierungstypen gruppiert angezeigt. |
| Entscheidungsrichtlinie | Entscheidungsrichtlinie, nach der die Attestierer für die Attestierungsobjekte ermittelt werden sollen. |
| Eigentümer | Ersteller der Attestierungsrichtlinie. Standardmäßig wird der Name des am One Identity Manager angemeldeten Benutzers eingetragen. Der Eigentümer kann geändert werden. |
| Bearbeitungszeit [Tage] | Anzahl der Tage, innerhalb derer die Attestierung entschieden sein soll. Wenn Sie die Bearbeitungszeit nicht festlegen möchten, erfassen Sie **0**.<br>Der One Identity Manager gibt nicht vor, welche Aktionen ausgeführt werden, wenn die Bearbeitungszeit überschritten ist. Definieren Sie für diesen Fall unternehmensspezifische Aktionen oder Auswertungen. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |
| Risikoindex | Gibt das Risiko für das Unternehmen an, wenn Attestierungen für diese Attestierungsrichtlinie abgelehnt werden. Stellen Sie über den Schieberegler einen Wert zwischen **0** und **1** ein.<br>• **0**: kein Risiko<br>• **1**: Die abgelehnte Attestierung ist ein Problem.<br>Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER \| CalculateRiskIndex** aktiviert ist. |
| Risikoindex (reduziert) | Gibt den Risikoindex unter Berücksichtigung der zugewiesenen risikomindernden Maßnahmen an. Der Risikoindex einer Attestierungsrichtlinie wird um die Werte **Signifikanzminderung** aller zugewiesenen risikomindernden Maßnahmen reduziert.<br>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. |

| Eigenschaft | Beschreibung |
|---|---|
| Zeitplan der Berechnung | Zeitplan, nach dem die Attestierung durchgeführt werden soll. Attestierungsvorgänge werden automatisch zu den Terminen erstellt, die im Zeitplan festgelegt sind. |
| Deaktiviert | Angabe, ob die Attestierungsrichtlinie deaktiviert ist.<br>Für deaktivierte Attestierungsrichtlinien werden keine Attestierungsvorgänge angelegt und somit keine Attestierungen durchgeführt. Deaktivierte Attestierungsrichtlinien können gelöscht werden.<br>Abgeschlossene Attestierungsvorgänge können gelöscht werden, sobald die Attestierungsrichtlinie deaktiviert wird. |
| Veraltete Vorgänge automatisch schließen | Angabe, ob offene Attestierungsvorgänge abgebrochen werden sollen, wenn neue angelegt werden.<br>Wenn eine Attestierung gestartet wird und die Option aktiviert ist, werden neue Attestierungsvorgänge entsprechend der Bedingung erstellt. Alle noch offenen, veralteten Attestierungsvorgänge für erneut ermittelte Attestierungsobjekte dieser Attestierungsrichtlinie werden abgebrochen. Attestierungsvorgänge für Attestierungsobjekte, die nicht erneut ermittelt wurden, bleiben erhalten. |
| Anzahl veralteter Vorgänge | Gibt die maximale Anzahl abgeschlossener Attestierungsvorgänge pro Attestierungsobjekt an, die in der Datenbank verbleiben sollen, wenn abgeschlossene Attestierungsvorgänge gelöscht werden.<br>• **0**: Es werden keine Attestierungsvorgänge gelöscht.<br>• **> 0**: Die angegebene Anzahl an abgeschlossenen Attestierungsvorgängen je Attestierungsobjekt verbleibt in der Datenbank. |
| Begründung der Entscheidung | Begründungstext, der angegeben wird, wenn die Option **Veraltete Vorgänge automatisch schließen** aktiviert ist und unbearbeitete Attestierungsvorgänge automatisch geschlossen werden. |
| Ausgabeformat | Format, in dem der Bericht erzeugt werden soll.<br>Die Auswahlliste ist nur sichtbar, wenn der Konfigurationsparameter **QER \| Attestation \| AllowAllReportTypes** aktiviert ist. Ist der Konfigurationsparameter nicht aktiviert, wird standardmäßig das PDF-Format genutzt, da dies als einziges Format revisionssicher ist. |
| Bedingung bearbeiten... | Startet den Where-Klausel-Assistenten. Mit diesem können Sie die Bedingung erstellen, welche die Attestierungsobjekte aus |

| Eigenschaft | Beschreibung |
|---|---|
| | der im Attestierungsverfahren festgelegten Datenbanktabelle ermittelt. |
| Bedingung | Datenbankabfrage, über die die Attestierungsobjekte ermittelt werden.<br>Das Eingabefeld ist nur sichtbar, wenn zuvor die Aufgabe **Bedingung anzeigen** ausgeführt wurde. |
| Attestierung mit Multifaktor-Authentifizierung | Attestierungen dieser Attestierungsrichtlinie erfordern eine Multifaktor-Authentifizierung. |

HINWEIS: Attestierungsrichtlinien, die im Web Portal erstellt wurden, können nur im Web Portal bearbeitet werden. Auf dem Stammdatenformular erscheint ein entsprechender Hinweis, wenn die Attestierungsrichtlinie im Web Portal erstellt wurde.

Wenn Sie eine solche Attestierungsrichtlinie im Manager bearbeiten möchten, erstellen Sie eine Kopie.

Ausführliche Informationen zum Bearbeiten einer Attestierungsrichtlinie im Web Portal finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

### Detaillierte Informationen zum Thema

- Bedingung anzeigen oder ausblenden auf Seite 35
- Zeitpläne auf Seite 19
- Attestierungsrichtlinien deaktivieren auf Seite 37
- Risikomindernde Maßnahmen auf Seite 153
- Einrichten der Multifaktor-Authentifizierung für Attestierungen auf Seite 89
- Kopie erstellen auf Seite 36

### Verwandte Themen

- Attestierungsvorgänge löschen auf Seite 108
- Attestierungsrichtlinien löschen auf Seite 37

# Risikobewertung

Mit dem One Identity Manager können Sie die Risiken von Attestierungsvorgängen bewerten. Dazu legen Sie an den Attestierungsrichtlinien einen Risikoindex fest. Der Risikoindex gibt an, welches Risiko mit der zu attestierenden Datensituation verbunden ist. Der Risikoindex wird als numerischer Wert mit dem Wertebereich 0 .. 1 angegeben. Dabei

legen Sie fest, ob mit den zu attestierenden Daten kein Risiko verbunden ist (Risikoindex = 0) oder ob jede Ablehnung ein Problem darstellt (Risikoindex = 1).

Durch geeignete Kontrollmaßnahmen kann das Risiko gesenkt werden, dass Attestierungsvorgänge abgelehnt werden. Diese Maßnahmen können als risikomindernde Maßnahmen im One Identity Manager erfasst werden. Der Wert, um den das Risiko gesenkt wird, wird als Signifikanzminderung an der risikomindernden Maßnahme angegeben. Mit diesem Wert wird der reduzierte Risikoindex der Attestierungsrichtlinien berechnet.

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

Risikobewertungen sind möglich, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.

### Detaillierte Informationen zum Thema

- Risikomindernde Maßnahmen auf Seite 153

# Standard-Attestierungsrichtlinien

Für die standardmäßige Attestierung neuer Benutzer sowie die Rezertifizierung aller in der One Identity Manager-Datenbank gespeicherten Personen stellt der One Identity Manager Standard-Attestierungsrichtlinien bereit. Darüber hinaus werden Standard-Attestierungsrichtlinien bereitgestellt, über die verschiedene Rollen, Mitgliedschaften in Rollen, Benutzerkonten und im Unified Namespace abgebildete Systemberechtigungen attestiert werden können.

***Um Standard-Attestierungsrichtlinien anzuzeigen***

- Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien | Vordefiniert**.

Für Standard-Attestierungsrichtlinien können folgende Eigenschaften unternehmensspezifisch geändert werden:

- Entscheidungsrichtlinie (wenn mehrere Entscheidungsrichtlinien zugeordnet werden können)
- Eigentümer
- Bearbeitungszeit
- Risikoindex
- Zeitplan der Berechnung
- Deaktiviert
- Veraltete Vorgänge automatisch schließen

- Anzahl veralteter Vorgänge
- Begründung der Entscheidung

TIPP: Wenn Sie die Attestierungsobjekte für Standard-Attestierungsrichtlinien unternehmensspezifisch einschränken wollen, erstellen Sie eine Kopie der Standard-Attestierungsrichtlinie. An der Kopie können Sie die Bedingung bearbeiten.

HINWEIS: Attestierungsrichtlinien, deren Bedingung als Definition (XML) hinterlegt ist, bearbeiten Sie im Web Portal. Die Definition (XML) kann im Manager nicht bearbeitet werden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

# Zusätzliche Aufgaben für Attestierungsrichtlinien

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

## Überblick über die Attestierungsrichtlinie

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

***Um einen Überblick über eine Attestierungsrichtlinie zu erhalten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie.
3. Wählen Sie die Aufgabe **Überblick über die Attestierungsrichtlinie**.

## Entscheider zuweisen

Über diese Aufgabe weisen Sie der ausgewählten Attestierungsrichtlinie die Personen zu, die als Entscheider in einem Attestierungsvorgang ermittelt werden können.

***Um Entscheider an eine Attestierungsrichtlinie zuzuweisen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie.
3. Wählen Sie die Aufgabe **Entscheider zuweisen**.

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

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

***Um eine Zuweisung zu entfernen***

- Wählen Sie den Entscheider und doppelklicken Sie .

4. Speichern Sie die Änderungen.

### Detaillierte Informationen zum Thema

- Auswahl der verantwortlichen Attestierer auf Seite 62

# Compliance Framework zuweisen

Über diese Aufgabe legen Sie fest, welche Compliance Frameworks für die ausgewählte Attestierungsrichtlinie 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 Attestierungsrichtlinie zuzuweisen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie.
3. Wählen Sie die Aufgabe **Compliance Frameworks zuweisen**.

   Weisen Sie im Bereich **Zuordnungen hinzufügen** die Compliance Frameworks zu.

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

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie das Compliance Framework und doppelklicken Sie .

4. Speichern Sie die Änderungen.

# Risikomindernde Maßnahmen

Risikomindernde Maßnahmen beschreiben Maßnahmen, die umgesetzt werden sollen, wenn eine Attestierung abgelehnt wurde. Nach Umsetzung der Maßnahmen sollte die Attestierung im nächsten Attestierungslauf genehmigt werden können.

***Um risikomindernde Maßnahmen zu bearbeiten***

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

### Detaillierte Informationen zum Thema

- Risikomindernde Maßnahmen auf Seite 153
- Risikomindernde Maßnahmen zuweisen auf Seite 34
- Risikomindernde Maßnahmen erstellen auf Seite 34

## Risikomindernde Maßnahmen zuweisen

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

***Um risikomindernde Maßnahmen an eine Attestierungsrichtlinie zuzuweisen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie.
3. Wählen Sie die Aufgabe **Risikomindernde Maßnahmen zuweisen**.

   Weisen Sie im Bereich **Zuordnungen hinzufügen** die risikomindernden Maßnahmen zu.

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

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die risikomindernden Maßnahme und doppelklicken Sie .
4. Speichern Sie die Änderungen.

## Risikomindernde Maßnahmen erstellen

***Um eine risikomindernde Maßnahme für Attestierungsrichtlinien zu erstellen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste eine Attestierungsrichtlinie.
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 **Attestierungsrichtlinien zuweisen**.
8. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die Attestierungsrichtlinien, die zugewiesen werden sollen.
9. Speichern Sie die Änderungen.

### Detaillierte Informationen zum Thema

- Risikomindernde Maßnahmen auf Seite 153

# Attestierung für einzelne Objekte starten

Mit dieser Aufgabe können Sie Attestierungen unabhängig vom Zeitplan starten. Wenn Sie die Aufgabe ausführen, wird ein separates Fenster geöffnet. In diesem wählen Sie aus der Liste aller Attestierungsobjekte die Objekte aus, die aktuell attestiert werden sollen. Die Auswahl gilt nur einmalig.

Für die ausgewählten Attestierungsobjekte wird die Option **Veraltete Vorgänge automatisch schließen** nicht berücksichtigt.

***Um Attestierungen für ausgewählte Objekte zu starten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie die Aufgabe **Attestierungsvorgänge für einzelne Objekte jetzt erstellen**.

   Ein separates Fenster wird geöffnet.
4. Aktivieren Sie in der Spalte **Attestierung** jedes Objekt, für das die Attestierung durchgeführt werden soll.
5. Klicken Sie **Starten**.

   Für die ausgewählten Attestierungsobjekte werden Attestierungsvorgänge erstellt. Sobald der DBQueue Prozessor den Auftrag bearbeitet hat, sehen Sie die neu erstellten Attestierungsvorgänge in der Navigationsansicht unter dem Menüeintrag **Attestierungsläufe | <Attestierungsrichtlinie> | Attestierungsläufe | <Jahr> | <Monat> | <Tag> | Offene Attestierungen**.
6. Klicken Sie **Schließen**.

# Bedingung anzeigen oder ausblenden

Die Bedingung, die die Attestierungsobjekte ermittelt, wird im Where-Klausel-Assistenten angezeigt und bearbeitet. Die SQL-Abfrage dieser Bedingung kann auf dem Stammdatenformular angezeigt werden.

***Um die Bedingung zur Ermittlung der Attestierungsobjekte auf dem Stammdatenformular anzuzeigen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

3. Wählen Sie die Aufgabe **Bedingung anzeigen**.

   Auf dem Stammdatenformular wird das Eingabefeld **Bedingung** angezeigt. Die Bedingung ist als Where-Klausel für Datenbankabfragen formuliert. Sie kann direkt bearbeitet werden.

***Um die Bedingung zur Ermittlung der Attestierungsobjekte auszublenden***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Wählen Sie die Aufgabe **Bedingung ausblenden**.

   Das Eingabefeld **Bedingung** wird nicht weiter auf dem Stammdatenformular angezeigt.

# Kopie erstellen

Von Attestierungsrichtlinien können Kopien erstellt werden. Kopien können Sie beispielsweise nutzen, um Standard-Attestierungsrichtlinien unternehmensspezifisch anzupassen.

***Um eine Attestierungsrichtlinie zu kopieren***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie.
3. Wählen Sie die Aufgabe **Kopie erstellen**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Auf dem Stammdatenformular wird die Kopie der Attestierungsrichtlinie mit der Bezeichnung **<Bezeichnung der originalen Attestierungsrichtlinie> (Kopie)** angezeigt. Sie können diese Attestierungsrichtlinie bearbeiten.

# Zeige ausgewählte Objekte

***Um eine Liste der ermittelten Attestierungsobjekte anzuzeigen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Wählen Sie die Aufgabe **Zeige ausgewählte Objekte**.

   Auf dem Stammdatenformular wird ein zusätzlicher Tabreiter **Ergebnis** eingeblendet. Dieser zeigt eine Liste aller Attestierungsobjekte, die über die Bedingung ermittelt werden.

# Attestierungsrichtlinien löschen

WICHTIG: Aus Gründen der Revisionssicherheit sollten Sie Attestierungsrichtlinien nicht löschen!

Attestierungsrichtlinien können dennoch unter bestimmten Voraussetzungen aus der One Identity Manager Datenbank entfernt werden. Stellen Sie dafür sicher, dass Attestierungsrichtlinien beim Löschen archiviert werden.

Ausführliche Informationen zur Datenarchivierung finden Sie im *One Identity Manager Konfigurationshandbuch*.

***Voraussetzung***

- Die Attestierungsrichtlinie ist deaktiviert.

***Um eine Attestierungsrichtlinie zu löschen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien | Deaktivierte Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Wählen Sie die Aufgabe **Attestierungsrichtlinie löschen**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Die Attestierungsrichtlinie wird gelöscht. Dabei werden alle verbundenen Attestierungsvorgänge, die Entscheidungsverläufe und die Attestierungshistorien gelöscht.

### Verwandte Themen

- Attestierungsrichtlinien deaktivieren auf Seite 37

# Attestierungsrichtlinien deaktivieren

Attestierungen werden durchgeführt, wenn der Zeitplan, der einer Attestierungsrichtlinie zugeordnet ist, aktiviert ist. Um zu verhindern, dass für einzelne Attestierungsrichtlinien Attestierungsvorgänge erstellt werden, können Sie die Attestierungsrichtlinien deaktivieren.

TIPP: Mit dem One Identity Manager werden zahlreiche Standard-Attestierungsrichtlinien ausgeliefert. Wenn Sie Ihre Datenbank für die Attestierung einrichten, überprüfen Sie, welche der Standard-Attestierungsrichtlinien für Ihre Datensituation relevant sind. Deaktivieren Sie alle nicht-benötigten Attestierungsrichtlinien.

***Um eine Attestierungsrichtlinie zu deaktivieren***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Aktivieren Sie **Deaktiviert**.
4. Speichern Sie die Änderungen.

# Unternehmensspezifische Mailvorlagen für Benachrichtigungen

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

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

# Mailtemplates für Attestierungen erstellen und ändern

***Um Mailvorlagen zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Mailvorlagen**.

   In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für Attestierungsvorgänge 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.

### Detaillierte Informationen zum Thema

- Allgemeine Eigenschaften einer Mailvorlage auf Seite 39
- Erstellen und Bearbeiten einer Maildefinition auf Seite 40

# Allgemeine Eigenschaften einer Mailvorlage

Für eine Mailvorlage werden die folgenden allgemeinen Eigenschaften abgebildet.

**Tabelle 10: Eigenschaften einer Mailvorlage**

| Eigenschaft | Bedeutung |
|---|---|
| Mailvorlage | Bezeichnung der Mailvorlage. Mit dieser Bezeichnung werden die Mailvorlagen in den Administrationswerkzeugen und im Web Portal angezeigt. Übersetzen Sie den eingegebenen Text über die Schaltfläche . |
| Basisobjekt | Basisobjekt der Mailvorlage. Die Angabe eines Basisobjekts ist nur erforderlich, wenn in der Maildefinition Eigenschaften des Basisobjekts referenziert werden.<br>Für Benachrichtigungen zur Attestierung verwenden Sie die Basisobjekte `AttestationCase` oder `AttestationHelper`. |
| Bericht (Parametersatz) | Bericht, der über die Mailvorlage zur Verfügung gestellt wird. |
| Beschreibung | Beschreibung der Mailvorlage. Übersetzen Sie den eingegebenen Text über die Schaltfläche . |
| Zielformat | Format, in dem die E-Mail Benachrichtigung generiert wird. Zulässige Werte sind:<br>• **HTML**: Die E-Mail Benachrichtigung wird als HTML formatiert. Im HTML-Format können Textformatierungen wie beispielsweise unterschiedliche Schriftarten, farbige Schriften oder andere Textformatierungen enthalten sein.<br>• **TXT**: Die E-Mail Benachrichtigung wird als Text formatiert. Das Text-Format unterstützt keine fetten, kursiven oder farbige Schriften oder andere Textformatierungen. Bilder, die direkt in der Benachrichtigung angezeigt werden, werden ebenfalls nicht unterstützt. |
| Designtyp | Design, in welchem die E-Mail Benachrichtigung generiert wird. Zulässige Werte sind:<br>• **Mailvorlage**: Die generierte E-Mail Benachrichtigung enthält den Mailbody entsprechend der Maildefinition. |

| Eigenschaft | Bedeutung |
|---|---|
| | • **Bericht**: Die generierte E-Mail Benachrichtigung enthält den unter **Bericht (Parametersatz)** angegebenen Bericht als Mailbody.<br>• **Mailvorlage, Bericht im Anhang**: Die generierte E-Mail Benachrichtigung enthält den Mailbody entsprechend der Maildefinition. Der unter **Bericht (Parametersatz)** angegebene Bericht wird als PDF-Datei an die Benachrichtigung angehängt. |
| Wichtigkeit | Wichtigkeit für die E-Mail Benachrichtigung. Zulässig sind die Werte **Niedrig**, **Normal** und **Hoch**. |
| Vertraulichkeit | Vertraulichkeit für die E-Mail Benachrichtigung. Zulässig sind die Werte **Normal**, **Persönlich**, **Privat** und **Vertraulich**. |
| Abbestellen erlaubt | Angabe, ob ein Empfänger die E-Mail Benachrichtigung abbestellen kann. Ist die Option aktiviert, kann die E-Mail Benachrichtigung über das Web Portal abbestellt werden. |
| Deaktiviert | Angabe, ob diese Mailvorlage deaktiviert ist. |
| Maildefinition | Eindeutige Bezeichnung der Maildefinition. |
| Sprachkultur | Sprachkultur, für welche die Mailvorlage gelten soll. Bei Generierung einer E-Mail-Benachrichtigung werden die Spracheinstellungen des Empfängers berücksichtigt. |
| Betreff | Betreff der E-Mail Benachrichtigung. |
| Mailbody | Inhalt der E-Mail Benachrichtigung. |

# Erstellen und Bearbeiten einer Maildefinition

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

***Um eine neue Maildefinition zu erstellen***

1. Öffnen Sie die Mailvorlage im Mailvorlageneditor.
2. Klicken Sie die Schaltfläche neben der Auswahlliste **Maildefinition**.
3. Wählen Sie in der Auswahlliste **Sprachkultur** die Sprache, für welche die Maildefinition gelten soll.

   Angezeigt werden alle Sprachen, die aktiviert sind. Um weitere Sprachen zu verwenden, aktivieren Sie im Designer die entsprechenden Länder. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.
4. Erfassen Sie im Eingabefeld **Betreff** die Betreffzeile.
5. Bearbeiten Sie in der Ansicht **Maildefinition** den Mailbody mit Hilfe des

Mailtexteditors.

6. Speichern Sie die Änderungen.

***Um eine vorhandene Maildefinition zu bearbeiten***

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

# Eigenschaften des Basisobjekts verwenden

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

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

## Beispiel

Ein Attestierer soll eine E-Mail Benachrichtigung mit neuen Aufträgen zur Attestierung erhalten.

**Tabelle 11: Eigenschaften einer E-Mail Benachrichtigung**

| Eigenschaft | Wert |
|---|---|
| Basisobjekt | AttestationHelper |
| Betreff | Neue Aufträge zur Attestierung |
| Mailbody | Sehr geehrte(r) $FK(UID_PersonHead).Salutation[D]$ $FK(UID_PersonHead).LastName$,<br>es liegen neue Aufträge zur Attestierung der Attestierungsrichtlinie "$FK(UID_AttestationCase).UID_AttestationPolicy[D]$" vor.<br>Erstellt: $FK(UID_AttestationCase).PolicyProcessed:Date$<br>Sie können den Auftrag im "One Identity Manager Self Service Portal" einsehen.<br>Mit freundlichen Grüßen |

# Verwenden von Hyperlinks zum Web Portal

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

***Voraussetzung für die Nutzung dieses Verfahrens***

- Der Konfigurationsparameter **QER | WebPortal | BaseURL** ist aktiviert und enthält den URL-Pfad zum Web Portal. Den Konfigurationsparameter bearbeiten Sie im Designer.

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

  mit:

  `<Servername> = Name des Servers`

  `<Anwendung> = Pfad zum Web Portal Installationsverzeichnis`

***Um einen Hyperlink zum Web Portal im Mailbody einzufügen***

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

     HINWEIS: Der One Identity Manager stellt einige Standardfunktionen zur Verfügung, welche Sie für die Erstellung von Hyperlinks zum Web Portal verwenden können.
3. Um die Eingaben zu übernehmen, klicken Sie **OK**.

# Standardfunktionen für die Erstellung von Hyperlinks

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

## Direkte Eingabe einer Funktion

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

`$Script(<Funktion>)$`

Beispiel:

```
$Script(VI_BuildAttestationLink_Approve)$
```

### Standardfunktionen für die Attestierung

Das Skript `VI_BuildAttestationLinks` enthält eine Sammlung von Standardfunktionen, um Hyperlinks für die direkte Attestierung aus E-Mail-Benachrichtigungen zusammenzusetzen.

**Tabelle 12: Funktionen des Skriptes `VI_BuildAttestationLinks`**

| Funktion | Verwendung |
|---|---|
| VI_BuildAttestationLink_Show | Öffnet die Seite zur Attestierung im Web Portal. |
| VI_BuildAttestationLink_Approve | Genehmigt eine Attestierung und öffnet die Seite zur Attestierung im Web Portal. |
| VI_BuildAttestationLink_Deny | Lehnt eine Attestierung ab und öffnet die Seite zur Attestierung im Web Portal. |
| VI_BuildAttestationLink_AnswerQuestion | Öffnet die Seite zum Beantworten einer Anfrage im Web Portal. |
| VI_BuildAttestationLink_Pending | Öffnet die Seite mit offenen Attestierungen im Web Portal. |

# Anpassen der E-Mail Signatur

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

**Tabelle 13: Konfigurationsparameter für die E-Mail Signatur**

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

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

# Mailtemplates für Attestierungen kopieren

***Um eine Mailvorlage zu kopieren***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Mailvorlagen**.

   In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für Attestierungsvorgänge 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**.

# Vorschau von Mailvorlagen für Attestierungen anzeigen

***Um die Vorschau einer Mailvorlage anzuzeigen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Mailvorlagen**.

   In der Ergebnisliste werden genau die Mailvorlagen angezeigt, die für Attestierungsvorgänge 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**.

# Mailvorlagen für Attestierungen löschen

***Um eine Mailvorlage zu löschen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Mailvorlagen**.

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

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

# Unternehmensspezifische Prozesse für Benachrichtigungen

Um innerhalb eines Attestierungsvorgangs weitere E-Mail Benachrichtigungen zu versenden, richten Sie unternehmensspezifische Prozesse ein. Folgende Ereignisse können Sie für die Generierung der Prozesse nutzen.

**Tabelle 14: Ereignisse am Objekt `AttestationHelper`**

| Ereignis | Ausgelöst durch |
|---|---|
| DecisionRequired | Erstellung eines neuen Attestierungsvorgangs<br>Wechsel zur nächsten Entscheidungsebene |
| Remind | Ablauf des Erinnerungsintervalls |

**Tabelle 15: Ereignisse am Objekt `AttestationCase`**

| Ereignis | Ausgelöst durch |
|---|---|
| Granted | Genehmigung eines Entscheidungsschrittes |
| Dismissed | Ablehnung eines Entscheidungsschrittes |
| OrderGranted | Genehmigung des gesamten Entscheidungsverfahrens |
| FinalDismissed | Ablehnung des gesamten Entscheidungsverfahrens |
| QueryToPerson | Stellen einer Anfrage |
| AnswerFromPerson | Beantworten einer Anfrage |
| RecallQuery | Zurückrufen einer Anfrage |
| Escalate | Eskalation des Attestierungsvorgangs |
| Aborted | Abbruch des Attestierungsvorgangs |
| Canceled | Abbruch veralteter Attestierungsvorgänge |

Ausführliche Informationen zum Erstellen von Prozessen finden Sie im *One Identity Manager Konfigurationshandbuch*.

# 2

# Genehmigungsverfahren für Attestierungsvorgänge

Alle Attestierungsvorgänge durchlaufen ein definiertes Genehmigungsverfahren. Während dieses Genehmigungsverfahrens entscheiden autorisierte Personen positiv oder negativ über die Attestierungsobjekte. Diese Genehmigungsverfahren können Sie variabel gestalten und somit an Ihre unternehmensspezifischen Richtlinien anpassen.

Für Genehmigungsverfahren definieren Sie Entscheidungsrichtlinien und Entscheidungsworkflows. In Entscheidungsrichtlinien legen Sie fest, welche Entscheidungsworkflows auf die Attestierungsvorgänge angewendet werden sollen. Über Entscheidungsworkflows ermitteln Sie, welche Personen, in welcher Reihenfolge die Attestierung genehmigen oder ablehnen können. Ein Entscheidungsworkflow kann mehrere Entscheidungsebenen und diese mehrere Entscheidungsschritte enthalten. In jedem Entscheidungsschritt werden über spezielle Entscheidungsverfahren die verantwortlichen Attestierer ermittelt.

### Detaillierte Informationen zum Thema


- Entscheidungsrichtlinien für Attestierungen auf Seite 46
- Entscheidungsworkflows für Attestierungen auf Seite 49
- Entscheidungsebenen bearbeiten auf Seite 54
- Standard-Entscheidungsverfahren auf Seite 63


# Entscheidungsrichtlinien für Attestierungen

Über Entscheidungsrichtlinien ermittelt der One Identity Manager die Attestierer für die einzelnen Attestierungsvorgänge.

***Um eine Entscheidungsrichtlinie zu bearbeiten***

1. Wählen Sie die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste eine Entscheidungsrichtlinie und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

# Allgemeine Stammdaten von Entscheidungsrichtlinien

Folgende Stammdaten erfassen Sie für eine Entscheidungsrichtlinie. Für eine neue Entscheidungsrichtlinie erfassen Sie mindestens Daten in den Pflichteingabefeldern.

**Tabelle 16: Allgemeine Stammdaten einer Entscheidungsrichtlinie**

| Eigenschaft | Beschreibung |
|---|---|
| Entscheidungsrichtlinie | Bezeichnung der Entscheidungsrichtlinie |
| Entscheidungsworkflow | Workflow, durch den die Attestierer ermittelt werden.<br>Wählen Sie einen beliebigen Entscheidungsworkflow aus der Auswahlliste aus oder klicken Sie , um einen neuen Entscheidungsworkflow einzurichten. |
| Mailvorlagen | Mailvorlage, die für die Erzeugung von E-Mail Benachrichtigungen bei Genehmigung, Ablehnung, Verlängerung, Abbestellung, Fristablauf oder Abbruch einer Attestierung verwendet wird. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |

## Detaillierte Informationen zum Thema

- Entscheidungsworkflows einrichten auf Seite 53
- Benachrichtigungen im Attestierungsvorgang auf Seite 110

# Standard-Entscheidungsrichtlinien für Attestierung

Für die standardmäßige Attestierung neuer Benutzer sowie die Rezertifizierung aller in der One Identity Manager-Datenbank gespeicherten Personen stellt der One Identity Manager eine Standard-Entscheidungsrichtlinie bereit. Darüber hinaus werden Standard-Entscheidungsrichtlinien bereitgestellt, über die verschiedene Rollen und im Unified Namespace abgebildete Systemberechtigungen attestiert werden können. Diese Standard-Entscheidungsrichtlinien können Sie nutzen, wenn Sie im Web Portal Attestierungsrichtlinien erstellen.

***Um Standard-Entscheidungsrichtlinien zu bearbeiten***

- Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsrichtlinien | Vordefiniert**.

Ausführliche Informationen zur Nutzung der Standard-Entscheidungsrichtlinien finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

### Verwandte Themen

- Attestierung und Rezertifizierung von Benutzern auf Seite 136
- Standardattestierungen und der Entzug von Berechtigungen auf Seite 126

# Zusätzliche Aufgaben für Entscheidungsrichtlinien

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

## Entscheidungsworkflow bearbeiten

Hier können Sie den Entscheidungsworkflow, welcher der Entscheidungsrichtlinie zugeordnet ist, bearbeiten.

***Um den zugeordneten Entscheidungsworkflow zu bearbeiten***

1. Wählen Sie die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Entscheidungsrichtlinie.
3. Wählen Sie die Aufgabe **1. Entscheidungsworkflow bearbeiten**.

   Der Workfloweditor wird geöffnet.

### Detaillierte Informationen zum Thema

- Arbeiten mit dem Workfloweditor auf Seite 50

## Auf Fehler untersuchen

Wenn Sie eine Entscheidungsrichtlinie bearbeitet haben, sollten Sie diese auf ihre Gültigkeit prüfen. Dabei wird geprüft, ob die Entscheidungsschritte in den Entscheidungsworkflows in ihrer Kombination zulässig sind. Unzulässige Entscheidungsschritte werden im Fehlermeldungsfenster ausgegeben.

***Um eine Entscheidungsrichtlinie zu prüfen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Entscheidungsrichtlinie.
3. Wählen Sie die Aufgabe **Auf Fehler untersuchen**.

# Entscheidungsworkflows für Attestierungen

Damit die Attestierer ermittelt werden können, müssen Sie den Entscheidungsrichtlinien einen Entscheidungsworkflow zuordnen. In einem Entscheidungsworkflow legen Sie Entscheidungsverfahren, die Anzahl der Attestierer und eine Bedingung für die Auswahl der Attestierer fest.

Entscheidungsworkflows erstellen und bearbeiten Sie mit dem Workfloweditor.

***Um einen Entscheidungsworkflow zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsworkflows**.
2. Wählen Sie in der Ergebnisliste den Entscheidungsworkflow und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

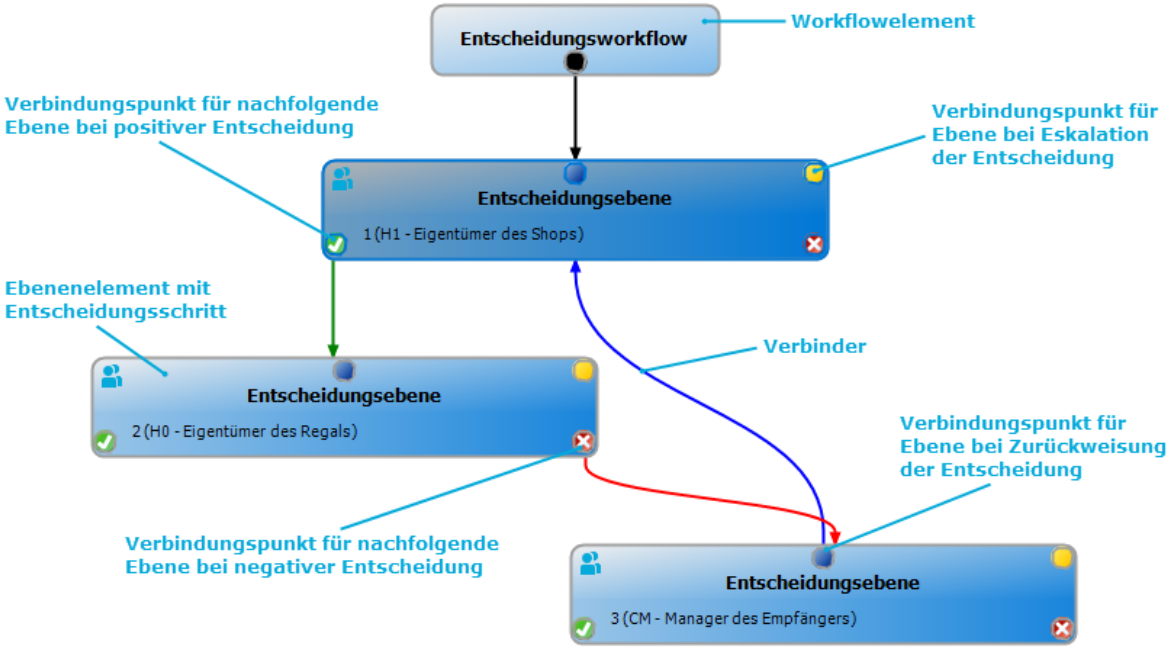
   Klicken Sie in der Ergebnisliste .

   Der Workfloweditor wird geöffnet.
3. Bearbeiten Sie den Entscheidungsworkflow.
4. Speichern Sie die Änderungen.

# Arbeiten mit dem Workfloweditor

Entscheidungsworkflows erstellen und bearbeiten Sie mit dem Workfloweditor. Der Workfloweditor erlaubt die Verkettung von Entscheidungsebenen. Mehrstufige Genehmigungsverfahren werden grafisch anschaulich dargestellt.

**Abbildung 1: Workfloweditor**




Im Workfloweditor werden die Entscheidungsebenen und die Entscheidungsschritte eines Entscheidungsworkflows über spezielle Steuerelemente dargestellt und bearbeitet. Der Workfloweditor verfügt über eine eigene Toolbox. Die Methoden der Toolbox werden abhängig von ihrer Anwendbarkeit auf das ausgewählte Steuerelement aktiviert und deaktiviert. Die Layoutposition der Steuerelemente im Workfloweditor können Sie mausgesteuert verändern oder automatisch anordnen lassen.

**Tabelle 17: Einträge in der Toolbox**

| Steuerelement | Methode | Bedeutung |
|---|---|---|
| Workflow | Bearbeiten | Die Eigenschaften des Entscheidungsworkflows werden bearbeitet. |
| | Automatisch anordnen | Die Workflowelemente werden automatisch angeordnet. Damit wird das Layout des Workflows neu bestimmt. |
| Entscheidungsebenen | Hinzufügen | Eine neue Entscheidungsebene wird zum Workflow hinzugefügt. |

| Steuerelement | Methode | Bedeutung |
|---|---|---|
| | Bearbeiten | Die Eigenschaften der Entscheidungsebene werden bearbeitet. |
| | Löschen | Die Entscheidungsebene wird gelöscht. |
| Entscheidungsschritte | Hinzufügen | Ein neuer Entscheidungsschritt wird zur Entscheidungsebene hinzugefügt. |
| | Bearbeiten | Die Eigenschaften des Entscheidungsschrittes werden bearbeitet. |
| | Löschen | Der Entscheidungsschritt wird gelöscht. |
| Zuordnungen | Positiv entfernen | Der Verbinder **Genehmigung** der ausgewählten Entscheidungsebene wird gelöscht. |
| | Negativ entfernen | Der Verbinder **Ablehnung** der ausgewählten Entscheidungsebene wird gelöscht. |
| | Umleitung entfernen | Der Verbinder **Umleitung** der ausgewählten Entscheidungsebene wird gelöscht. |
| | Eskalation entfernen | Der Verbinder **Eskalation** der ausgewählten Entscheidungsebene wird gelöscht. |

Jedes der Steuerelemente besitzt ein Eigenschaftsfenster, über das Sie die Daten des Entscheidungsworkflows, der Entscheidungsebene oder des Entscheidungsschrittes bearbeiten. Das Eigenschaftsfenster öffnen Sie über die Methode **Toolbox | <Steuerelement> | Bearbeiten**.

Um ein Steuerelement zu löschen, markieren Sie das Element und wählen Sie die Methode **Toolbox | <Steuerelement> | Löschen**.

Die einzelnen Elemente verketten Sie über Verbinder miteinander. Die Verbindungspunkte aktivieren Sie mausgesteuert. Bei der Auswahl eines Verbindungspunktes wechselt der Mauszeiger zum Pfeilsymbol. Halten Sie die linke Maustaste gedrückt und ziehen Sie einen Verbinder von einem Verbindungspunkt zum zweiten Verbindungspunkt.

**Abbildung 2: Verbinder im Entscheidungsworkflow**

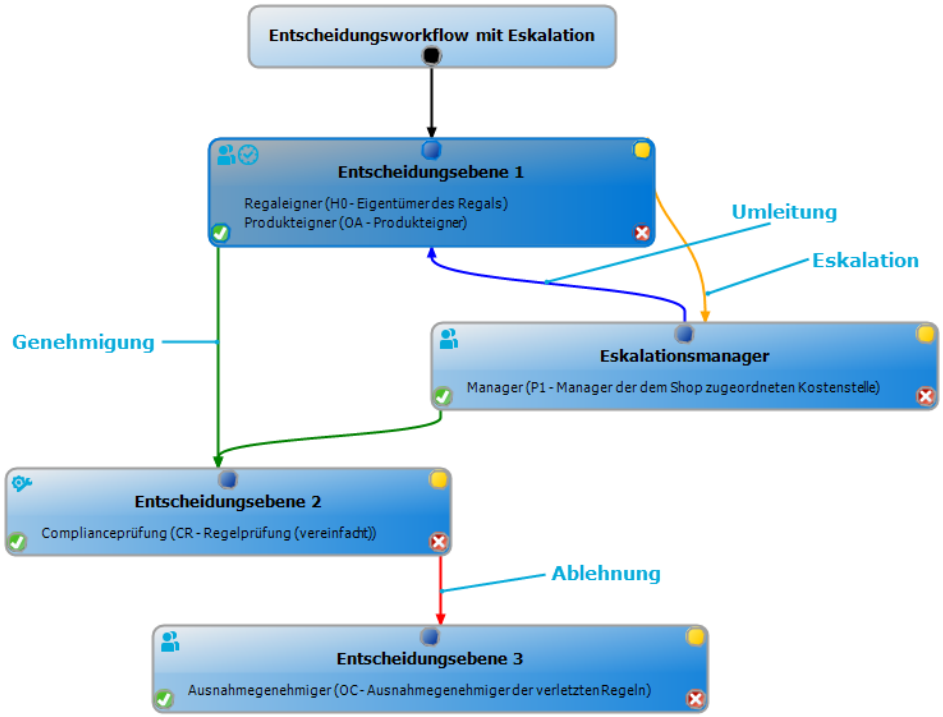



**Tabelle 18: Verbinder im Entscheidungsworkflow**

| Verbinder | Bedeutung |
|---|---|
| Genehmigung | Verbindung zur nachfolgenden Entscheidungsebene, wenn die aktuelle Entscheidungsebene positiv entschieden wurde. |
| Ablehnung | Verbindung zur nachfolgenden Entscheidungsebene, wenn die aktuelle Entscheidungsebene negativ entschieden wurde. |
| Umleitung | Verbindung zu einer beliebigen Entscheidungsebene, um die aktuelle Entscheidung umzuleiten. |
| Eskalation | Verbindung zu einer beliebigen Entscheidungsebene, wenn die aktuelle Entscheidung bei Timeout eskaliert werden soll. |

Standardmäßig wird beim Einfügen der ersten Entscheidungsebene sofort eine Verbindung zwischen Workflowelement und Ebenenelement hergestellt. Soll die Hierarchie der Ebenen geändert werden, können Sie mit der Maus einen neuen Verbinder zu einem anderen Ebenenelement ziehen.

Verbinder zwischen den Ebenenelementen können Sie alternativ über die Methoden **Toolbox | Zuordnungen** lösen. Markieren Sie dafür das Ebenenelement, an dem der Verbinder startet. Anschließend fügen Sie einen neuen Verbinder ein.

Auf den Ebenenelementen werden abhängig von der Konfiguration der Entscheidungsschritte verschiedene Symbole dargestellt.

**Tabelle 19: Symbole auf einem Ebenenelement**

| Symbol | Bedeutung |
|---|---|
|  | Die Entscheidung wird vom System vorgenommen. |
|  | Die Entscheidung wird manuell vorgenommen. |
|  | Der Entscheidungsschritt enthält eine Erinnerungsfunktion. |
|  | Der Entscheidungsschritt enthält ein Timeout-Intervall. |

Änderungen an den einzelnen Elementen übernehmen Sie erst durch das Speichern des gesamten Entscheidungsworkflows. Zusätzlich zum Inhalt des Entscheidungsworkflows wird auch die Layoutposition der einzelnen Elemente im Workfloweditor gespeichert.

# Entscheidungsworkflows einrichten

Ein Entscheidungsworkflow besteht aus einer oder mehreren Entscheidungsebenen. Eine Entscheidungsebene kann einen Entscheidungsschritt oder mehrere parallele Entscheidungsschritte umfassen. Innerhalb des Attestierungsverfahrens müssen alle Entscheidungsschritte einer Entscheidungsebene durchlaufen werden, bevor die nächste Entscheidungsebene aufgerufen wird. Die Abfolge der Entscheidungsebenen im Entscheidungsworkflow wird über Verbinder hergestellt.

Wenn Sie einen neuen Entscheidungsworkflow erstellen, wird zunächst ein neues Workflowelement erzeugt.

***Um die Eigenschaften eines Entscheidungsworkflows zu bearbeiten***

1. Öffnen Sie den Workfloweditor.
2. Wählen Sie die Methode **Toolbox | Workflow | Bearbeiten**.
3. Bearbeiten Sie die Eigenschaften des Workflows.
4. Klicken Sie **OK**.

**Tabelle 20: Eigenschaften eines Entscheidungsworkflows**

| Eigenschaft | Bedeutung |
|---|---|
| Bezeichnung | Bezeichnung des Entscheidungsworkflows. |
| Systemabbruch (Tage) | Anzahl der Tage, nach deren Ablauf der Entscheidungsworkflow, und somit das gesamte Attestierungsverfahren, automatisch durch das System beendet wird. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |

### Detaillierte Informationen zum Thema

- Abbruch eines Attestierungsvorgangs bei Zeitüberschreitung auf Seite 98

# Entscheidungsebenen bearbeiten

Eine Entscheidungsebene dient zur Gruppierung einzelner Entscheidungsschritte. Alle Entscheidungsschritte einer Entscheidungsebene werden zeitlich parallel ausgeführt. Alle Entscheidungsschritte verschiedener Entscheidungsebenen werden zeitlich nacheinander ausgeführt. Die Reihenfolge legen Sie über die Verbinder fest.

In den Entscheidungsebenen legen Sie die einzelnen Entscheidungsschritte fest. Pro Entscheidungsebene ist mindestens ein Entscheidungsschritt notwendig. Wenn Sie eine Entscheidungsebene hinzufügen, erfassen Sie zuerst die erforderlichen Entscheidungsschritte.

***Um eine Entscheidungsebene einzufügen***

1. Wählen Sie die Methode **Toolbox | Entscheidungsebenen | Hinzufügen**.

   Das Eigenschaftsfenster für den ersten Entscheidungsschritt wird geöffnet.
2. Erfassen Sie die Eigenschaften des Entscheidungsschritts.
3. Speichern Sie die Änderungen.

Sobald Sie eine Entscheidungsebene mit mindestens einem Entscheidungsschritt erstellt haben, können Sie die Eigenschaften dieser Entscheidungsebene bearbeiten.

***Um die Eigenschaften einer Entscheidungsebene zu bearbeiten***

1. Markieren Sie die Entscheidungsebene.
2. Wählen Sie die Methode **Toolbox | Entscheidungsebenen | Bearbeiten**.
3. Erfassen Sie den Anzeigenamen der Entscheidungsebene.
4. Speichern Sie die Änderungen.

HINWEIS: Sie können mehrere Entscheidungsschritte auf einer Entscheidungsebene definieren. Die Attestierer einer Entscheidungsebene können in diesem Fall für einen Attestierungsvorgang parallel, statt nacheinander, entscheiden. Erst wenn innerhalb des Attestierungsverfahrens alle Entscheidungsschritte einer Entscheidungsebene abgeschlossen sind, wird der Attestierungsvorgang den Attestierern der nächsten Entscheidungsebene vorgelegt.

***Um weitere Entscheidungsschritte in eine Entscheidungsebene einzufügen***

1. Markieren Sie die Entscheidungsebene.
2. Wählen Sie die Methode **Toolbox | Entscheidungsschritte | Hinzufügen**.
3. Erfassen Sie die Eigenschaften des Entscheidungsschritts.
4. Speichern Sie die Änderungen.

### Verwandte Themen

- Eigenschaften eines Entscheidungsschritts auf Seite 55
- Entscheidungsschritte bearbeiten

# Entscheidungsschritte bearbeiten

***Um die Eigenschaften eines Entscheidungsschritts zu bearbeiten***

1. Markieren Sie den Entscheidungsschritt.
2. Wählen Sie die Methode **Toolbox | Entscheidungsschritte | Bearbeiten**.
3. Bearbeiten Sie die Eigenschaften des Entscheidungsschritts.
4. Speichern Sie die Änderungen.

### Detaillierte Informationen zum Thema

- Eigenschaften eines Entscheidungsschritts auf Seite 55

# Eigenschaften eines Entscheidungsschritts

Auf dem Tabreiter **Allgemein** erfassen Sie die folgenden Daten. Auf dem Tabreiter **Mailvorlagen** wählen Sie die Mailvorlagen für die Erzeugung von E-Mail Benachrichtigungen aus. Für einen neuen Entscheidungsschritt erfassen Sie mindestens die Daten in den Pflichteingabefeldern.

**Tabelle 21: Allgemeine Eigenschaften eines Entscheidungsschritts**

| Eigenschaft | Bedeutung |
|---|---|
| Einzelschritt | Bezeichnung des Entscheidungsschrittes |
| Entscheidungsverfahren | Anzuwendendes Verfahren zur Ermittlung der Attestierer. |
| Rolle | Hierarchische Rolle, aus der die Attestierer mit den Standard-Entscheidungsverfahren OM und OR ermittelt werden sollen. |
| Fallback-Entscheider | Anwendungsrolle, deren Mitglieder berechtigt sind, die Attestierungsvorgänge zu entscheiden, wenn durch das Entscheidungsverfahren kein Attestierer ermittelt werden kann. Weisen Sie eine Anwendungsrolle aus der Auswahlliste zu.<br>Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*. |

| Eigenschaft | Bedeutung |
| --- | --- |
| | HINWEIS: Die Anzahl der Entscheider wird nicht auf die Fallback-Entscheider angewendet. Der Entscheidungsschritt gilt als entschieden, sobald 1 Fallback-Entscheider entschieden hat. |
| Bedingung | Bedingung für die Berechnung der Entscheidung mit den Entscheidungsverfahren CD, EX oder WC. |
| Anzahl Entscheider | Anzahl der Attestierer, die einen Attestierungsvorgang entscheiden müssen. Mit dieser Angabe schränken Sie die maximale Anzahl der Entscheider des eingesetzten Entscheidungsverfahrens weiter ein.<br>Wenn für einen Entscheidungsschritt mehrere Personen als Attestierer ermittelt werden, dann bestimmt die hier angegebene Anzahl, wie viele Personen dieses Personenkreises einen Attestierungsvorgang entscheiden müssen. Erst danach wird der Attestierungsvorgang den Attestierern der nächsten Ebene vorgelegt.<br>Können nicht genügend Attestierer ermittelt werden, wird der Entscheidungsschritt den Fallback-Entscheidern vorgelegt. Der Entscheidungsschritt gilt als entschieden, sobald 1 Fallback-Entscheider den Attestierungsvorgang entschieden hat.<br>Sollen alle über das eingesetzte Entscheidungsverfahren ermittelten Personen entscheiden, beispielsweise alle Mitglieder einer Rolle (Standardentscheidungsverfahren OR), dann geben Sie den Wert **-1** an. Damit wird die am Entscheidungsverfahren definierte maximale Anzahl an Attestierern außer Kraft gesetzt.<br>In den Entscheidungsverfahren CD, EX oder WC wird eine am Entscheidungsschritt definierte Anzahl der Entscheider nicht berücksichtigt. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |
| Begründung Genehmigung | Begründung, die bei einer positiven automatischen Entscheidung in den Attestierungsvorgang eingetragen wird.<br>Das Eingabefeld wird nur für die Entscheidungsverfahren CD, EX und WC angezeigt. |
| Begründung Ablehnung | Begründung, die bei einer negativen automatischen Entscheidung in den Attestierungsvorgang und die Attestierungshistorie eingetragen wird.<br>Das Eingabefeld wird nur für die Entscheidungsverfahren CD, EX und WC angezeigt. |
| Erinnerung nach | Anzahl der Arbeitsstunden, nach deren Ablauf die Attestierer |

| Eigenschaft | Bedeutung |
| --- | --- |
| (Arbeitsstunden) | per E-Mail Benachrichtigung erinnert werden, dass noch offene Attestierungsvorgänge zur Attestierung vorliegen.<br><br>Das Erinnerungsintervall wird standardmäßig alle 30 Minuten geprüft. Um dieses Prüfintervall zu ändern, passen Sie den Zeitplan **Erinnerungsintervall und Timeout von Attestierungsvorgängen prüfen** an.<br><br>HINWEIS: Für die Ermittlung der gültigen Arbeitszeiten stellen Sie sicher, dass in den Stammdaten der Personen ein Bundesland und/oder ein Bundesstaat eingetragen ist. Wenn diese Informationen fehlen, wird ein Fallback zur Berechnung der Arbeitszeit genutzt. Ausführliche Informationen zur Ermittlung der Arbeitszeit von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.<br><br>Wurden mehrere Attestierer ermittelt, dann erhält jeder Attestierer die Benachrichtigung. Gleiches gilt, wenn ein zusätzlicher Attestierer beauftragt wurde.<br><br>Hat ein Attestierer die Entscheidung delegiert, wird der Zeitpunkt für die Erinnerung für den Empfänger der Delegierung neu berechnet. Der Empfänger der Delegierung und alle übrigen Attestierer erhalten die Benachrichtigung. Der ursprüngliche Attestierer wird nicht benachrichtigt.<br><br>Wenn ein Attestierer eine Anfrage gestellt hat, wird der Zeitpunkt für die Erinnerung für die angefragte Person neu berechnet. Solange die Anfrage nicht beantwortet ist, erhält nur diese Person die Benachrichtigung. |
| Timeout (Arbeitsstunden) | Anzahl der Arbeitsstunden, nach deren Ablauf der Entscheidungsschritt automatisch entschieden wird.<br><br>Das Timeout wird standardmäßig alle 30 Minuten geprüft. Um das Prüfintervall zu ändern, passen Sie den Zeitplan **Erinnerungsintervall und Timeout von Attestierungsvorgängen prüfen** an.<br><br>Für die Zeitberechnung wird die gültige Arbeitszeit des jeweiligen Entscheiders berücksichtigt. |

| Eigenschaft | Bedeutung |
| --- | --- |
| | HINWEIS: Für die Ermittlung der gültigen Arbeitszeiten stellen Sie sicher, dass in den Stammdaten der Personen ein Bundesland und/oder ein Bundesstaat eingetragen ist. Wenn diese Informationen fehlen, wird ein Fallback zur Berechnung der Arbeitszeit genutzt. Ausführliche Informationen zur Ermittlung der Arbeitszeit von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.<br><br>Wurden mehrere Entscheider ermittelt, dann wird der Entscheidungsschritt erst dann automatisch entschieden, wenn der Timeout für alle Entscheider überschritten ist. Gleiches gilt, wenn ein zusätzlicher Entscheider beauftragt wurde.<br><br>Hat ein Entscheider die Entscheidung delegiert, wird der Zeitpunkt für die automatische Entscheidung für den neuen Entscheider neu berechnet. Wenn dieser die Entscheidung zurückweist, wird der Zeitpunkt für die automatische Entscheidung für den ursprünglichen Entscheider neu berechnet.<br><br>Wenn ein Entscheider eine Anfrage stellt, muss die Entscheidung trotzdem innerhalb des definierten Timeouts getroffen werden. Der Zeitpunkt für die automatische Entscheidung wird nicht neu berechnet. |
| Verhalten bei Timeout | Aktion, die im Falle einer Zeitüberschreitung ausgeführt wird.<br><br>• **Genehmigung**: Der Attestierungsvorgang wird in diesem Entscheidungsschritt genehmigt. Es wird die nächste Entscheidungsebene aufgerufen.<br>• **Ablehnung**: Der Attestierungsvorgang wird in diesem Entscheidungsschritt abgelehnt. Es wird die Entscheidungsebene für Ablehnung aufgerufen.<br>• **Eskalation**: Der Attestierungsvorgang wird eskaliert. Es wird die Entscheidungsebene zur Eskalation aufgerufen.<br>• **Abbruch**: Der Entscheidungsschritt, und somit das gesamte Attestierungsverfahren, wird abgebrochen. |
| Zusätzliche Entscheider erlaubt | Gibt an, ob ein aktueller Attestierer eine weitere Person als Attestierer beauftragen darf. Dieser zusätzliche Attestierer ist für den aktuellen Attestierungsvorgang parallel entscheidungsberechtigt. Erst wenn beide Entscheidungen abgeschlossen sind, wird der Attestierungsvorgang den Attestierern der nächsten Ebene vorgelegt. |

| Eigenschaft | Bedeutung |
| --- | --- |
| | Die Option kann nur für Entscheidungsebenen mit einem einzelnen, manuellen Entscheidungsschritt aktiviert werden. |
| Entscheidung delegierbar | Gibt an, ob ein aktueller Attestierer die Attestierung an eine andere Person delegieren darf. Diese Person wird als Attestierer in den aktuellen Entscheidungsschritt aufgenommen. Sie entscheidet anstelle des delegierenden Attestierers.<br>Die Option kann nur für Entscheidungsebenen mit einem einzelnen, manuellen Entscheidungsschritt aktiviert werden. |
| Entscheidung durch betroffene Person | Gibt an, ob die Person, die von der Entscheidung betroffen ist, diesen Attestierungsvorgang auch entscheiden darf. Ist die Option aktiviert, können die zu attestierenden Personen sich selbst attestieren.<br>Ist die Option deaktiviert, legen Sie am Konfigurationsparameter **QER \| Attestation \| PersonToAttestNoDecide** für alle Attestierungen fest, ob die zu attestierenden Personen sich selbst attestieren dürfen. |
| Nicht in Genehmigungshistorie anzeigen | Gibt an, ob der Entscheidungsschritt in der Attestierungshistorie ausgeblendet werden soll. Beispielsweise kann dieses Verhalten für Entscheidungsschritte mit dem Entscheidungsverfahren **CD - Errechnete Entscheidung** eingesetzt werden, die nur zur Verzweigung im Entscheidungsbaum dienen. Es erhöht die Übersichtlichkeit der Attestierungshistorie. |

## Detaillierte Informationen zum Thema

- Benachrichtigungen im Attestierungsvorgang auf Seite 110
- Erinnerung der Attestierer auf Seite 112
- Eskalieren eines Attestierungsvorgangs auf Seite 93
- Automatische Entscheidung bei Zeitüberschreitung auf Seite 96
- Abbruch eines Attestierungsvorgangs bei Zeitüberschreitung auf Seite 98
- Attestierer über eine festgelegte Rolle ermitteln auf Seite 75
- Errechnete Entscheidung auf Seite 77
- Extern vorzunehmende Entscheidung auf Seite 78
- Warten auf andere Entscheidung auf Seite 79
- Attestierung durch die zu attestierende Person verhindern auf Seite 90

## Verwandte Themen

- Auswahl der verantwortlichen Attestierer auf Seite 62
- Attestierer können nicht ermittelt werden auf Seite 95

- Attestierungen durch die zentrale Entscheidergruppe auf Seite 100

# Entscheidungsebenen verbinden

Wenn Sie Entscheidungsworkflows mit mehreren Entscheidungsebenen einrichten, müssen Sie die einzelnen Ebenen miteinander verbinden. Dabei können Sie folgende Verknüpfungen erstellen:

**Tabelle 22: Verknüpfungen für Entscheidungsebenen**

| Verknüpfung | Beschreibung |
|---|---|
| Genehmigung | Verbindung zur nachfolgenden Entscheidungsebene, wenn die aktuelle Entscheidungsebene positiv entschieden wurde. |
| Ablehnung | Verbindung zur nachfolgenden Entscheidungsebene, wenn die aktuelle Entscheidungsebene negativ entschieden wurde. |
| Umleitung | Verbindung zu einer beliebigen Entscheidungsebene, um die aktuelle Entscheidung umzuleiten.<br>Attestierer können die Entscheidung durch eine andere Entscheidungsebene ausführen lassen, beispielsweise wenn im Einzelfall die Entscheidung durch einen Manager erforderlich ist. Erstellen Sie dafür eine Verbindung zu der Entscheidungsebene, an die eine Entscheidung umgeleitet werden kann. Auf diesem Weg können Entscheidungen auch an eine vorhergehende Entscheidungsebene zurückgegeben werden, beispielsweise bei unzureichender Begründung einer Entscheidung.<br>Nicht möglich sind Umleitungen an Entscheidungsschritte mit den Entscheidungsverfahren EX, CD, SB oder WC. |
| Eskalation | Verbindung zu einer beliebigen Entscheidungsebene, wenn die aktuelle Entscheidung bei Zeitüberschreitung eskaliert werden soll. |

Sind keine nachfolgenden Entscheidungsebenen zur aktuellen Entscheidungsebene angegeben, dann gilt bei einer positiven Entscheidung der Attestierungsvorgang als genehmigt. Bei einer negativen Entscheidung gilt der Attestierungsvorgang dann als endgültig abgelehnt. Das Attestierungsverfahren ist in beiden Fällen abgeschlossen.

# Zusätzliche Aufgaben für Entscheidungsworkflows

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

# Überblick über den Entscheidungsworkflow

***Um einen Überblick über einen Entscheidungsworkflow zu erhalten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsworkflows**.
2. Wählen Sie in der Ergebnisliste den Entscheidungsworkflow.
3. Wählen Sie die Aufgabe **Überblick über den Entscheidungsworkflow**.

# Entscheidungsworkflow kopieren

Um beispielsweise Standard-Entscheidungsworkflows unternehmensspezifisch anzupassen, können Sie Entscheidungsworkflows kopieren und anschließend bearbeiten.

***Um einen Entscheidungsworkflow zu kopieren***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsworkflows**.
2. Wählen Sie in der Ergebnisliste einen Entscheidungsworkflow und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Wählen Sie die Aufgabe **Workflow kopieren**.
4. Erfassen Sie eine Bezeichnung für die Kopie.
5. Klicken Sie **Ok**, um die Kopieraktion zu starten.

   - ODER -

   Klicken Sie **Abbrechen**, um die Kopieraktion abzubrechen.
6. Um die Kopie sofort zu bearbeiten, klicken Sie **Ja**.

   - ODER -

   Um die Kopie später zu bearbeiten, klicken Sie **Nein**.

# Entscheidungsworkflow löschen

Ein Entscheidungsworkflow kann nur gelöscht werden, wenn er keiner Entscheidungsrichtlinie zugeordnet ist.

***Um einen Entscheidungsworkflow zu löschen***

1. Entfernen Sie alle Zuordnungen zu Entscheidungsrichtlinien.
   a. Prüfen Sie, welchen Entscheidungsrichtlinien der Entscheidungsworkflow zugeordnet ist.

b. Wechseln Sie auf das Stammdatenformular der Entscheidungsrichtlinie und ordnen Sie einen anderen Entscheidungsworflow zu.

2. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsworkflows**.
3. Wählen Sie in der Ergebnisliste einen Entscheidungsworkflow.
4. Klicken Sie .
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

### Detaillierte Informationen zum Thema

- Überblick über den Entscheidungsworkflow auf Seite 61
- Allgemeine Stammdaten von Entscheidungsrichtlinien auf Seite 47

# Standard-Entscheidungsworkflows

Für die standardmäßige Attestierung neuer Benutzer sowie die Rezertifizierung aller in der One Identity Manager-Datenbank gespeicherten Personen stellt der One Identity Manager einen Standard-Entscheidungsworkflow bereit. Darüber hinaus werden Standard-Entscheidungsworkflows bereitgestellt, über die verschiedene Rollen und im Unified Namespace abgebildete Systemberechtigungen attestiert werden können. Diese Standard-Entscheidungsrichtlinien können Sie nutzen, wenn Sie im Web Portal Attestierungsrichtlinien erstellen.

***Um Standard-Entscheidungsworkflows zu bearbeiten***

- Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsworkflows | Vordefiniert**.

Ausführliche Informationen zur Nutzung der Standard-Entscheidungsworkflows finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

### Verwandte Themen

- Attestierung und Rezertifizierung von Benutzern auf Seite 136
- Standardattestierungen und der Entzug von Berechtigungen auf Seite 126

# Auswahl der verantwortlichen Attestierer

Der One Identity Manager kann die Entscheidungen in einem Attestierungsverfahren automatisch treffen oder durch Attestierer treffen lassen. Ein Attestierer ist eine Person oder eine Gruppe von Personen, die innerhalb eines Attestierungsverfahrens einen

Attestierungsvorgang genehmigen oder ablehnen kann. Wer die Entscheidungen trifft, wird über verschiedene Entscheidungsverfahren ermittelt. Welches Entscheidungsverfahren angewendet werden soll, wird am Entscheidungsschritt festgelegt.

Werden durch ein Entscheidungsverfahren mehrere Personen als Entscheider ermittelt, dann bestimmt die am Entscheidungsschritt angegebene Anzahl, wie viele Personen diesen Schritt entscheiden müssen. Erst danach wird der Attestierungsvorgang den Attestierern der nächsten Ebene vorgelegt. Kann für einen Entscheidungsschritt kein Entscheider ermittelt werden, wird das Attestierungsverfahren abgebrochen.

Der One Identity Manager stellt standardmäßig Entscheidungsverfahren bereit. Zusätzlich können Sie eigene Entscheidungsverfahren definieren.

Welche Person in welcher Entscheidungsebene entscheidungsberechtigt ist, wird durch den DBQueue Prozessor berechnet. Beachten Sie bei der Einrichtung von Entscheidungsworkflows die Besonderheiten der einzelnen Entscheidungsverfahren zur Ermittlung der entscheidungsberechtigten Personen.

# Standard-Entscheidungsverfahren

***Um Standard-Entscheidungsverfahren anzuzeigen***

- Wählen Sie die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsverfahren | Vordefiniert**.

Für die Auswahl der verantwortlichen Attestierer sind standardmäßig die nachfolgend aufgeführten Entscheidungsverfahren bereitgestellt.

**Tabelle 23: Entscheidungsverfahren für Attestierung**

| Bezeichnung des Verfahrens | Attestierer |
|---|---|
| AA - Attestierer der zu attestierenden Rolle | Attestierer der Organisation (Abteilung, Standort, Kostenstelle), Geschäftsrolle oder des IT Shops, wenn Zuweisungen von Systemberechtigungen oder Systemrollen an Rollen attestiert werden.<br>• Attestierer für Abteilungen, Kostenstellen und Standorte müssen der Anwendungsrolle **Identity Management \| Organisationen \| Attestierer** zugewiesen sein.<br>• Attestierer für Geschäftsrollen müssen der Anwendungsrolle **Identity Management \| Geschäftsrollen \| Attestierer** zugewiesen sein.<br>• Attestierer für Bestellungen müssen der Anwendungsrolle **Request & Fulfillment \| IT Shop \| Attestierer** zugewiesen sein.<br>Weitere Informationen finden Sie unter Attestierer über |

| Bezeichnung des Verfahrens | Attestierer |
|---|---|
| | Attestierungsobjekte ermitteln auf Seite 70. |
| AD - Attestierer der Abteilung des Empfängers | Attestierer der Abteilung, die dem Attestierungsobjekt primär zugeordnet ist.<br>• Attestierer für Abteilungen müssen der Anwendungsrolle **Identity Management \| Organisationen \| Attestierer** zugewiesen sein.<br>Weitere Informationen finden Sie unter Attestierer über die Rolle der zu attestierenden Person ermitteln auf Seite 69. |
| AL - Attestierer des Standorts des Empfängers | Attestierer des Standorts, der dem Attestierungsobjekt primär zugeordnet ist.<br>• Attestierer für Standorte müssen der Anwendungsrolle **Identity Management \| Organisationen \| Attestierer** zugewiesen sein.<br>Weitere Informationen finden Sie unter Attestierer über die Rolle der zu attestierenden Person ermitteln auf Seite 69. |
| AM - Manager der verbundenen Person | Manager der Person, die mit dem zu attestierenden Benutzerkonto verbunden ist.<br>Weitere Informationen finden Sie unter Verantwortliche der Attestierungsobjekte als Attestierer ermitteln auf Seite 73. |
| AN - Attestierer der zu attestierenden Systemberechtigung | Attestierer der Systemberechtigung oder Systemrolle, wenn Zuweisungen von Systemberechtigungen oder Systemrollen an Rollen attestiert werden. Die Attestierer werden über die zugeordnete Leistungsposition ermittelt.<br>• Attestierer müssen der Anwendungsrolle **Request & Fulfillment \| IT Shop \| Attestierer** zugewiesen sein.<br>Weitere Informationen finden Sie unter Attestierer über Attestierungsobjekte ermitteln auf Seite 70. |
| AO - Attestierer der primären Rolle des Empfängers | Attestierer der Geschäftsrolle, die dem Attestierungsobjekt primär zugeordnet ist.<br>Attestierer für Geschäftsrollen müssen der Anwendungsrolle **Identity Management \| Geschäftsrollen \| Attestierer** zugewiesen sein.<br>Weitere Informationen finden Sie unter Attestierer über |

| Bezeichnung des Verfahrens | Attestierer |
|---|---|
| | die Rolle der zu attestierenden Person ermitteln auf Seite 69. |
| AP - Attestierer der Kostenstelle des Empfängers | Attestierer der Kostenstelle, die dem Attestierungsobjekt primär zugeordnet ist.<br>• Attestierer für Kostenstellen müssen der Anwendungsrolle **Identity Management \| Organisationen \| Attestierer** zugewiesen sein.<br>Weitere Informationen finden Sie unter Attestierer über die Rolle der zu attestierenden Person ermitteln auf Seite 69. |
| AR - Attestierer der zu attestierenden Complianceregel | Attestierer der Complianceregel, die attestiert wird.<br>• Attestierer müssen der Anwendungsrolle **Identity & Access Governance \| Identity Audit \| Attestierer** zugewiesen sein.<br>Weitere Informationen finden Sie unter Attestierer über Attestierungsobjekte ermitteln auf Seite 70. |
| AS - Entscheider der Attestierungsrichtlinie | Alle Personen, die als Entscheider der Attestierungsrichtlinie zugewiesen sind.<br>Weitere Informationen finden Sie unter Attestierer über die Attestierungsrichtlinie ermitteln auf Seite 69. |
| AT - Attestierer der zu attestierenden Organisation | Attestierer der Organisation (Abteilung, Standort, Kostenstelle), Geschäftsrolle oder des IT Shops, die/der attestiert wird.<br>• Attestierer für Abteilungen, Kostenstellen und Standorte müssen der Anwendungsrolle **Identity Management \| Organisationen \| Attestierer** zugewiesen sein.<br>• Attestierer für Geschäftsrollen müssen der Anwendungsrolle **Identity Management \| Geschäftsrollen \| Attestierer** zugewiesen sein.<br>• Attestierer für Bestellungen müssen der Anwendungsrolle **Request & Fulfillment \| IT Shop \| Attestierer** zugewiesen sein.<br>Weitere Informationen finden Sie unter Attestierer über Attestierungsobjekte ermitteln auf Seite 70. |
| AY - Attestierer der zu attestierenden | Attestierer der Unternehmensrichtlinie, die attestiert wird. |

| Bezeichnung des Verfahrens | Attestierer |
|---|---|
| Unternehmensrichtlinie | • Attestierer müssen der Anwendungsrolle **Identity & Access Governance \| Unternehmensrichtlinien \| Attestierer** zugewiesen sein.<br>Weitere Informationen finden Sie unter Attestierer über Attestierungsobjekte ermitteln auf Seite 70. |
| CD - Errechnete Entscheidung | -<br>Weitere Informationen finden Sie unter Errechnete Entscheidung auf Seite 77. |
| CM - Manager des Empfängers | Manager der Person, die attestiert wird.<br>Weitere Informationen finden Sie unter Manager der Attestierungsobjekte als Attestierer ermitteln auf Seite 71. |
| DM - Abteilungsleiter des Empfängers | Manager/Stellvertreter der Abteilung, wenn Personen oder sekundäre Mitgliedschaften in Abteilungen attestiert werden.<br>Weitere Informationen finden Sie unter Manager der Attestierungsobjekte als Attestierer ermitteln auf Seite 71. |
| ED - Abteilungsleiter bei Attestierung einer Systemberechtigung | Abteilungsleiter der Person, deren Systemberechtigungen attestiert werden.<br>Weitere Informationen finden Sie unter Verantwortliche der Attestierungsobjekte als Attestierer ermitteln auf Seite 73. |
| EM - Manager der Person bei Attestierung einer Systemberechtigung | Manager der Person, deren Systemberechtigungen attestiert werden.<br>Weitere Informationen finden Sie unter Verantwortliche der Attestierungsobjekte als Attestierer ermitteln auf Seite 73. |
| EN - Zielsystemverantwortliche der zu attestierenden Systemberechtigung | Zielsystemverantwortliche der Systemberechtigung, die attestiert wird.<br>Weitere Informationen finden Sie unter Verantwortliche der Attestierungsobjekte als Attestierer ermitteln auf Seite 73. |
| EO - Produkteigner der zu attestierenden Systemberechtigung | Produkteigner, der Systemberechtigung oder der Systemrolle, die attestiert wird.<br>Weitere Informationen finden Sie unter Verantwortliche |

| Bezeichnung des Verfahrens | Attestierer |
|---|---|
| | der Attestierungsobjekte als Attestierer ermitteln auf Seite 73. |
| EX - Extern vorzunehmende Entscheidung | -<br>Weitere Informationen finden Sie unter Extern vorzunehmende Entscheidung auf Seite 78. |
| LM - Manager des Standorts | Manager/Stellvertreter des Standorts, wenn Personen oder sekundäre Mitgliedschaften in Standorten attestiert werden.<br>Weitere Informationen finden Sie unter Manager der Attestierungsobjekte als Attestierer ermitteln auf Seite 71. |
| MD - Manager der Abteilung der verbundenen Person | Manager der primären Abteilung der Person, die mit dem zu attestierenden Benutzerkonto verbunden ist.<br>Weitere Informationen finden Sie unter Verantwortliche der Attestierungsobjekte als Attestierer ermitteln auf Seite 73. |
| MO - Manager der Geschäftsrolle | Manager/Stellvertreter der Geschäftsrolle, wenn Personen oder sekundäre Mitgliedschaften in Geschäftsrollen attestiert werden.<br>Weitere Informationen finden Sie unter Manager der Attestierungsobjekte als Attestierer ermitteln auf Seite 71. |
| OA - Produkteigner | Alle Mitglieder der zugeordneten Anwendungsrolle, wenn Leistungspositionen, Systemberechtigungen oder Systemrollen attestiert werden.<br>Weitere Informationen finden Sie unter Produkteigner als Attestierer ermitteln auf Seite 75. |
| OM - Manager einer bestimmten Rolle | Manager der im Entscheidungsworkflow festgelegten Rolle.<br>Weitere Informationen finden Sie unter Attestierer über eine festgelegte Rolle ermitteln auf Seite 75. |
| OP - Eigentümer eines privilegierten Objektes | Alle Personen, die als Eigentümer der bestellten privilegierten Zugriffsanforderung ermittelt werden können.<br>Weitere Informationen finden Sie unter Eigentümer eines privilegierten Objektes als Attestierer ermitteln auf Seite 76. |

| Bezeichnung des Verfahrens | Attestierer |
|---|---|
| OR - Mitglieder einer bestimmten Rolle | Alle Personen, die der im Entscheidungsworkflow festgelegten Rolle sekundär zugewiesen sind.<br>Weitere Informationen finden Sie unter Attestierer über eine festgelegte Rolle ermitteln auf Seite 75. |
| PA - Zusätzlicher Besitzer der Active Directory Gruppe | Alle Personen, die über den zusätzlichen Besitzer der zu attestierenden Active Directory Gruppe ermittelt werden können.<br>Weitere Informationen finden Sie unter Zusätzlicher Besitzer einer Active Directory Gruppe als Attestierer ermitteln auf Seite 76. |
| PM - Kostenstellenverantwortliche des Empfängers | Verantwortlicher/Stellvertreter der Kostenstelle, wenn sekundäre Mitgliedschaften in Kostenstellen attestiert werden.<br>Weitere Informationen finden Sie unter Manager der Attestierungsobjekte als Attestierer ermitteln auf Seite 71. |
| PO - Vorgeschlagener Eigentümer | Vorgeschlagener Eigentümer des Attestierungsobjekts<br>Weitere Informationen finden Sie unter Eigentümer der Attestierungsobjekte als Attestierer ermitteln auf Seite 76. |
| RE - Verantwortlicher der zu attestierenden Systemrolle | Verantwortlicher der Systemrolle, die attestiert wird.<br>Weitere Informationen finden Sie unter Manager der Attestierungsobjekte als Attestierer ermitteln auf Seite 71. |
| RM - Manager der Rolle bei Attestierung von Mitgliedschaften | Manager der zu attestierenden Rolle, wenn sekundäre Mitgliedschaften in Rollen attestiert werden.<br>Weitere Informationen finden Sie unter Manager der Attestierungsobjekte als Attestierer ermitteln auf Seite 71. |
| RR - Manager der Rolle bei Attestierung von Rollen | Manager der zu attestierenden Rolle.<br>Weitere Informationen finden Sie unter Manager der Attestierungsobjekte als Attestierer ermitteln auf Seite 71. |
| SO - Zielsystemverantwortliche der zu attestierenden Berechtigung | Zielsystemverantwortliche der Systemberechtigung oder des Benutzerkontos, das attestiert wird.<br>Weitere Informationen finden Sie unter Verantwortliche der Attestierungsobjekte als Attestierer ermitteln auf |

| Bezeichnung des Verfahrens | Attestierer |
|---|---|
| | Seite 73. |
| WC - Warten auf andere Entscheidung | -<br>Weitere Informationen finden Sie unter Warten auf andere Entscheidung auf Seite 79. |

# Attestierer über die Attestierungsrichtlinie ermitteln

Wenn Sie die Attestierer für beliebige Objekte an einer Attestierungsrichtlinie festlegen wollen, nutzen Sie das Entscheidungsverfahren AS. Das Entscheidungsverfahren ermittelt alle Personen, die als Entscheider der Attestierungsrichtlinie zugewiesen sind.

Mit diesem Verfahren können Sie beliebige Objekte durch beliebige, festgelegte Personen attestieren lassen. Diese Personen müssen als Entscheider der Attestierungsrichtlinie zugewiesen sein. Die Attestierer können auch beim Erstellen von Attestierungsrichtlinien im Web Portal angegeben werden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

### Verwandte Themen

- Entscheider zuweisen auf Seite 32

# Attestierer über die Rolle der zu attestierenden Person ermitteln

Installierte Module: Geschäftsrollenmodul (für Entscheidungsverfahren AO)

Wenn Sie Zuweisungen von Unternehmensressourcen zu Ihren Mitarbeitern oder Bestellungen Ihrer Mitarbeiter attestieren wollen, nutzen Sie die Entscheidungsverfahren AD, AL, AO oder AP. Die ermittelten Attestierer sind Mitglied der Anwendungsrolle **Attestierer**.

Attestierungsobjekte sind Personen (Tabelle: `Person`) oder Empfänger einer Bestellung (Tabelle: `PersonWantsOrg`). Die Entscheidungsverfahren ermitteln zu jedem Attestierungsobjekt den Attestierer der Rolle (Abteilung, Standort, Geschäftsrolle, Kostenstelle), die dem Attestierungsobjekt primär zugeordnet ist. Ist der primär zugeordneten Rolle kein Attestierer direkt zugeordnet, ermittelt das Entscheidungsverfahren den Attestierer übergeordneter Rollen. Wird auch auf diesem Weg kein Attestierer gefunden, wird der Attestierungsvorgang dem Attestierer der zugehörigen Rollenklasse zur Entscheidung vorgelegt.

HINWEIS: Wenn die Attestierer über das Entscheidungsverfahren AO ermittelt werden und für die Geschäftsrollen Bottom-Up-Vererbung festgelegt ist, beachten Sie Folgendes:

- Wenn der primär zugeordneten Geschäftsrolle kein Attestierer zugeordnet ist, werden die Attestierer der untergeordneten Geschäftsrolle ermittelt.

### Verwandte Themen

- Standard-Entscheidungsverfahren auf Seite 63

# Attestierer über Attestierungsobjekte ermitteln

Wenn Sie die Gültigkeit von Complianceregeln, Regelverletzungen, Unternehmensrichtlinien, Richtlinienverletzungen oder Abteilungen, Standorten, Kostenstellen oder Geschäftsrollen attestieren wollen, nutzen Sie die Entscheidungsverfahren AR, AY oder AT. Das Verfahren AT eignet sich auch, um Zuweisungen an IT Shop-Strukturen (Shops, Shoppingcenter oder Regale) zu attestieren. Um Zuweisungen von Systemberechtigungen oder Systemrollen zu Abteilungen, Standorten, Kostenstellen, Geschäftsrollen oder IT Shop-Strukturen zu attestieren, nutzen Sie die Entscheidungsverfahren AA oder AN. Die ermittelten Attestierer sind Mitglied der Anwendungsrolle **Attestierer**.

| | **Basisobjekte der Attestierung** | **Verfügbar im Modul** |
|---|---|---|
| AR | Regeln (`ComplianceRule`)<br>Regelverletzungen (`PersonInNonCompliance`) | Modul Complianceregeln |
| AY | Unternehmensrichtlinien (`QERPolicy`)<br>Richtlinienverletzungen (`QERPolicyHasObject`) | Modul Unternehmensrichtlinien |
| AT | Abteilungen (`Department`)<br>IT Shop Strukturen (`ITShopOrg`)<br>Standorte (`Locality`)<br>Geschäftsrollen (`Org`)<br>Kostenstellen (`ProfitCenter`)<br>IT Shop Vorlagen (`ITShopSrc`) | |
| AA, AN | Zuweisungen von Systemberechtigungen oder Zielsystemgruppen an Rollen (`<BaseTree>HasUNSGroupB`, `<BaseTree>HasADSGroup`, `<BaseTree>HasEBSResp`, ...)<br>Zuweisungen von Systemrollen an Rollen (`<BaseTree>HasESet`) | Zielsystem Basismodul |

Die Entscheidungsverfahren ermitteln den Attestierer, der dem Attestierungsobjekt zugeordnet ist. Das Entscheidungsverfahren AA ermittelt den Attestierer über die Rolle (Abteilungen, Standorte, Geschäftsrollen, Kostenstellen) oder IT Shop Strukturen (IT Shop Vorlagen). Das Entscheidungsverfahren AN ermittelt den Attestierer über die Leistungsposition, die der Systemberechtigung beziehungsweise Zielsystemgruppe zugeordnet ist.

Für die Entscheidungsverfahren AT und AA gilt darüber hinaus: Ist dem Attestierungsobjekt kein Attestierer direkt zugeordnet, ermittelt das Entscheidungsverfahren den Attestierer übergeordneter Rollen/IT Shop Strukturen. Wird auch auf diesem Weg kein Attestierer gefunden, wird der Attestierungsvorgang dem Attestierer der zugehörigen Rollenklasse zur Entscheidung vorgelegt.

HINWEIS: Wenn das Basisobjekt der Attestierung eine Geschäftsrolle oder die Zuweisung an eine Geschäftsrolle ist und für die zugehörige Rollenklasse Bottom-Up-Vererbung festgelegt ist, beachten Sie Folgendes:

- Ist dem Attestierungsobjekt kein Attestierer direkt zugeordnet, ermittelt das Entscheidungsverfahren den Attestierer untergeordneter Rollen.

### Verwandte Themen

- Standard-Entscheidungsverfahren auf Seite 63

# Manager der Attestierungsobjekte als Attestierer ermitteln

Wenn Sie Personen, Benutzerkonten, Rollen, Systemrollen, Rollenmitgliedschaften, Zuweisungen von Systemrollen oder Systemberechtigungen an Personen, Rollen oder IT Shop Strukturen durch deren Manager attestieren lassen wollen, nutzen Sie die Entscheidungsverfahren CM, DM, LM, MO, RM, RR oder RE.

| Entscheidungsverfahren | Basisobjekte der Attestierung | Verfügbar im Modul |
|---|---|---|
| CM | Personen (`Person`)<br>Personen: Mitgliedschaften in Rollen und Organisationen (`PersonInBaseTree`) | |
| DM | Personen (`Person`)<br>Personen: Mitgliedschaften in Abteilungen (`PersonInDepartment`) | |
| LM | Personen (`Person`)<br>Personen: Mitgliedschaften in Standorten (`PersonInLocality`) | |

| Entscheidungsverfahren | Basisobjekte der Attestierung | Verfügbar im Modul |
|---|---|---|
| MO | Personen (Person)<br>Personen: Mitgliedschaften in Geschäftsrollen (PersonInOrg) | Geschäftsrollenmodul |
| PM | Personen (Person)<br>Personen: Mitgliedschaften in Kostenstellen (PersonInProfitCenter) | |
| RE | Systemrollen (ESet)<br>Personen: Zuweisungen Systemrollen (PersonHasESet)<br>Abteilungen: Zuweisungen Systemrollen (DepartmentHasESet)<br>Geschäftsrollen: Zuweisungen Systemrollen (OrgHasESet)<br>IT Shop Strukturen: Zuweisungen Systemrollen (ITShopOrgHasESet)<br>IT Shop Vorlagen: Zuweisungen Systemrollen (ITShopSrcHasESet)<br>Kostenstellen: Zuweisungen Systemrollen (ProfitCenterHasESet)<br>Standorte: Zuweisungen Systemrollen (LocalityHasESet) | Systemrollenmodul |
| RM | Personen: Mitgliedschaften in Abteilungen (PersonInDepartment)<br>Personen: Mitgliedschaften in IT Shop Strukturen (PersonInITShopOrg)<br>Personen: Mitgliedschaften in Standorten (PersonInLocality)<br>Personen: Mitgliedschaften in Geschäftsrollen (PersonInOrg)<br>Personen: Mitgliedschaften in Kostenstellen (PersonInProfitCenter) | |
| RR | Abteilungen (Department)<br>IT Shop Strukturen (ITShopOrg)<br>Standorte (Locality) | |

| Entscheidungsverfahren | Basisobjekte der Attestierung | Verfügbar im Modul |
|---|---|---|
| | Geschäftsrollen (`Org`)<br>Kostenstellen (`ProfitCenter`)<br>IT Shop Vorlagen (`ITShopSrc`)<br>alle Zuweisungen von Systemberechtigungen oder Systemrollen an Rollen; beispielsweise **Rollen und Organisationen: Zuweisungen Active Directory Gruppen** (`BaseTreeHasADSGroup`) oder **Standorte: Zuweisungen EBS Berechtigungen** (`LocalityHasEBSResp`) | |

Die Entscheidungsverfahren ermitteln zu jedem Attestierungsobjekt den Manager. Beim Entscheidungsverfahren RE wird der Verantwortliche der Systemrolle als Attestierer ermittelt, bei den Entscheidungsverfahren RM und RR der Manager der Rolle/IT Shop Struktur. Die Entscheidungsverfahren CM, DM, LM, MO und PM ermitteln den Manager und stellvertretenden Leiter der Rolle, in der die zu attestierende Person Mitglied ist.

# Verantwortliche der Attestierungsobjekte als Attestierer ermitteln

Wenn Sie Systemberechtigungen und die ihnen zugewiesenen Benutzerkonten attestieren wollen, nutzen Sie die Entscheidungsverfahren ED, EM, EN, EO oder SO. Für die Attestierung von Benutzerkonten nutzen Sie die Entscheidungsverfahren AM, MD oder SO.

Attestierungsobjekte sind Benutzerkonten oder Systemberechtigungen und die ihnen zugewiesenen Benutzerkonten sowie Systemrollen, denen Systemberechtigungen oder Systemrollen zugewiesen sind. Die Entscheidungsverfahren ermitteln die folgenden Attestierer:

| | Basisobjekte der Attestierung | Attestierer | Verfügbar im Modul |
|---|---|---|---|
| AM | Benutzerkonten (`UNSAccount`) | Manager der Person, mit der das Benutzerkonto verbunden ist. | Zielsystem Basis-modul |
| ED | Benutzerkonten: Zuweisungen an Systemberechtigungen (`UNSAccountInUNSGroup`) | Abteilungsleiter (und dessen Stellvertreter) der Person, mit der das Benut-zerkonto verbunden ist. Es | Zielsystem Basismodul |

| | Basisobjekte der Attestierung | Attestierer | Verfügbar im Modul |
|---|---|---|---|
| | | gilt die primär zugewiesene Abteilung. | |
| EM | Benutzerkonten: Zuweisungen an Systemberechtigungen (UNSAccountInUNSGroup) | Manager der Person, mit der das Benutzerkonto verbunden ist. | Zielsystem Basismodul |
| EN | Benutzerkonten: Zuweisungen an Systemberechtigungen (UNSAccountInUNSGroup)<br>Systemberechtigungen (UNSGroup) | Zielsystemverantwortliche des Zielsystembereichs, zu dem die Systemberechtigung gehört. | Zielsystem Basismodul |
| EO | Systemrollen: Zuweisungen (ESetHasEntitlement)<br>alle Zuweisungen von Benutzerkonten an Systemberechtigungen; beispielsweise **Benutzerkonten: Zuweisungen an Systemberechtigungen** (UNSAccountInUNSGroup) oder **SAP Benutzerkonten: Zuweisungen an Rollen** (SAPUserInSAPRole)<br>alle Zuweisungen von Systemberechtigungen oder Systemrollen an Rollen; beispielsweise **Rollen und Organisationen: Zuweisungen Active Directory Gruppen** (BaseTreeHasADSGroup) oder **Standorte: Zuweisungen EBS Berechtigungen** (LocalityHasEBSResp) | Produkteigner der Leistungsposition, die der Systemberechtigung oder der Systemrolle zugeordnet ist. | Zielsystem Basismodul oder Systemrollenmodul |
| MD | Benutzerkonten (UNSAccount) | Abteilungsleiter (und dessen Stellvertreter) der Person, mit der das Benutzerkonto verbunden ist. Es gilt die primär zugewiesene Abteilung. | Zielsystem Basismodul |
| SO | Benutzerkonten: Zuweisungen an Systemberechtigungen (UNSAccountInUNSGroup)<br>Benutzerkonten (UNSAccount)<br>Systemberechtigungen: Zuweisungen an Systemberechtigungen (UNSGroupInUNSGroup) | Zielsystemverantwortliche des Zielsystembereichs, zu dem die Systemberechtigung oder das Benutzerkonto gehört. | Zielsystem Basismodul |

# Attestierer über eine festgelegte Rolle ermitteln

Wenn die Attestierer für beliebige Objekte in einer bestimmten Rolle festgelegt sind, nutzen Sie die Entscheidungsverfahren OR oder OM. Mit diesen Entscheidungsverfahren können Sie beliebige Objekte durch Personen einer beliebigen Rolle attestieren lassen. Im Entscheidungsschritt legen Sie die Rolle fest, über welche die Attestierer ermittelt werden sollen. Die Entscheidungsverfahren ermitteln folgende Attestierer.

| | Auswählbare Rollen | Attestierer |
|---|---|---|
| OM | Abteilungen (`Department`)<br>Kostenstellen (`ProfitCenter`)<br>Standorte (`Locality`)<br>Geschäftsrollen (`Org`) | Manager und Stellvertreter der am Entscheidungsschritt festgelegten Rolle |
| OR | Abteilungen (`Department`)<br>Kostenstellen (`ProfitCenter`)<br>Standorte (`Locality`)<br>Geschäftsrollen (`Org`)<br>Anwendungsrollen (`AERole`) | Alle sekundären Mitglieder der am Entscheidungsschritt festgelegten Rolle |

# Produkteigner als Attestierer ermitteln

Wenn Produkteigner als Attestierer ermittelt werden sollen, nutzen Sie das Entscheidungsverfahren OA. Es können damit folgende Objekte attestiert werden:

- Leistungspositionen
- Systemberechtigungen
- Zuweisungen von Systemberechtigungen an Benutzerkonten oder Systemberechtigungen
- Zuweisungen von Systemrollen an Personen

Voraussetzungen:

- Den Systemberechtigungen und Systemrollen muss eine Leistungsposition zugeordnet sein.
- Der Leistungsposition muss eine Anwendungsrolle für Produkteigner zugeordnet sein.

Es werden alle Personen als Attestierer ermittelt, die der zugeordneten Anwendungsrolle zugewiesen sind.

## Eigentümer eines privilegierten Objektes als Attestierer ermitteln

Installierte Module: Privileged Account Governance Modul

Wenn Sie privilegierte Objekte eines Privileged Account Management Systems, wie beispielsweise PAM Assets oder PAM Verzeichniskonten, durch deren Eigentümer attestieren lassen wollen, nutzen Sie das Entscheidungsverfahren OP. Die Eigentümer attestieren den möglichen Zugriff von Benutzern auf diese privilegierten Objekte. Die Eigentümer der privilegierten Objekte müssen der Anwendungsrolle **Privileged Account Governance | Asset- und Konteneigentümer** oder einer untergeordneten Anwendungsrolle zugewiesen sein.

## Zusätzlicher Besitzer einer Active Directory Gruppe als Attestierer ermitteln

Installierte Module: Active Roles Modul

Wenn eine Active Directory Gruppe attestiert wird, können die Attestierer über die zusätzlichen Besitzer dieser Active Directory Gruppe ermittelt werden. Nutzen Sie dafür das Entscheidungsverfahren PA. Damit werden alle Personen ermittelt, die

- über ihr Active Directory Benutzerkonto Mitglied in der zugeordneten Active Directory Gruppe sind beziehungsweise
- die mit dem zugeordeten Active Directory Benutzerkonto verbunden sind.

HINWEIS: Nutzen Sie das Entscheidungsverfahren PA nur dann, wenn der Konfigurationsparameter **TargetSystem | ADS | ARS_SSM** aktiviert ist. Die Spalte **Zusätzliche Besitzer** ist nur in diesem Fall verfügbar.

## Eigentümer der Attestierungsobjekte als Attestierer ermitteln

Wenn Sie im Web Portal neue Eigentümer an Geräte oder Systemberechtigungen zuweisen, dann soll der neue Eigentümer dieser Zuweisung zustimmen. Dafür wird eine Attestierung mit dem Entscheidungsverfahren PO durchgeführt.

# Errechnete Entscheidung

HINWEIS: Pro Entscheidungsebene kann nur ein Entscheidungsschritt mit dem Entscheidungsverfahren CD definiert werden.

Wenn Sie den Verlauf einer Attestierung von bestimmten Bedingungen abhängig machen wollen, nutzen Sie das Entscheidungsverfahren CD. Dieses Verfahren ermittelt keine Attestierer. Der One Identity Manager trifft die Entscheidung abhängig von der Bedingung, die im Entscheidungsschritt formuliert ist.

Das Verfahren können Sie für beliebige Basisobjekte der Attestierung anwenden. Im Entscheidungsschritt erstellen Sie eine Bedingung. Liefert die Bedingung ein Ergebnis, wird der Entscheidungsschritt durch den One Identity Manager genehmigt. Liefert die Bedingung kein Ergebnis, wird der Entscheidungsschritt durch den One Identity Manager abgelehnt. Folgen darauf keine weiteren Entscheidungsschritte wird der Attestierungsvorgang endgültig genehmigt oder abgelehnt.

***Um eine Bedingung für das Entscheidungsverfahren CD zu erfassen***

1. Bearbeiten Sie die Eigenschaften des Entscheidungsschritts.

   Weitere Informationen finden Sie unter Entscheidungsebenen bearbeiten auf Seite 54.

2. Erfassen Sie im Eingabefeld **Bedingung** eine gültige Where-Klausel für Datenbankabfragen. Sie können diese direkt als SQL-Abfrage eingeben oder über einen Assistenten zusammenstellen. Auf den konkreten Attestierungsvorgang nehmen Sie in der Bedingung über die Variable `@UID_AttestationCase` Bezug.

## Beispiel für einen einfachen Entscheidungsworkflow mit Entscheidungsverfahren CD

Externe Personen sollen durch ihren Manager attestiert werden. Wenn kein Manager zugewiesen ist, sollen die Mitglieder einer festgelegten Anwendungsrolle die Personen attestieren.

Mit dem Entscheidungsverfahren CD und der folgenden Bedingung ermitteln Sie alle externen Personen, denen ein Manager zugeordnet ist.

```
EXISTS
(SELECT 1 FROM
     (SELECT xobjectkey FROM Person WHERE (IsExternal = 1)
     AND (EXISTS
     (SELECT 1 FROM
          (SELECT UID_Person FROM Person WHERE 1 = 1) as X
     WHERE X.UID_Person = Person.UID_PersonHead) )) as X
WHERE X.xobjectkey = AttestationCase.ObjectKeyBase)
```

Ist die Bedingung erfüllt, soll der Manager der externen Person die Person attestieren. Dafür ergänzen Sie im positiven Entscheidungspfad einen Entscheidungsschritt mit dem Entscheidungsverfahren CM.

Ist die Bedingung nicht erfüllt, sollen die Mitglieder einer festgelegten Anwendungsrolle die Person attestieren. Dafür ergänzen Sie im negativen Entscheidungspfad einen Entscheidungsschritt mit dem Entscheidungsverfahren OR und ordnen die Anwendungsrolle zu.

# Extern vorzunehmende Entscheidung

Wenn die Attestierung ausgeführt werden soll, sobald ein definiertes Ereignis außerhalb des One Identity Manager eintritt, nutzen Sie die extern vorzunehmende Entscheidung (Entscheidungsverfahren EX). Sie können dieses Verfahren auch nutzen, um beliebige Objekte durch Personen attestieren zu lassen, die keinen Zugriff auf den One Identity Manager haben.

Im Entscheidungsschritt legen Sie ein Ereignis fest, das eine externe Entscheidung auslöst. Durch das Ereignis wird ein Prozess angestoßen, der die externe Entscheidung für den Attestierungsvorgang initiiert und das Ergebnis der Entscheidung auswertet. Das Genehmigungsverfahren wartet, bis das Ergebnis der externen Entscheidung an den One Identity Manager übermittelt wird. Abhängig von dieser Entscheidung definieren Sie weitere Entscheidungsschritte.

***Um das Entscheidungsverfahren nutzen zu können***

1. Definieren Sie eigene Prozesse, die
    - eine externe Entscheidung auslösen,
    - die Ergebnisse der externen Entscheidung auswerten und
    - die daraufhin den externen Entscheidungsschritt im One Identity Manager positiv oder negativ entscheiden.
2. Definieren Sie ein Ereignis, das den Prozess für die externe Entscheidung startet. Erfassen Sie das Ereignis im Entscheidungsschritt im Eingabefeld **Ereignis**.

Ist das externe Ereignis eingetreten, muss der Status des Entscheidungsschrittes im One Identity Manager geändert werden. Nutzen Sie dafür die Prozessfunktion `CallMethod` mit der Methode `MakeDecision`. Übergeben Sie der Prozessfunktion folgende Parameter:

```
MethodName: Value = "MakeDecision"

ObjectType: Value = "AttestationCase"

Param1: Value = "sa"

Param2: Value = <Entscheidung> ("true" = zugestimmt; "false" = abgelehnt)

Param3: Value = <Begründung der Entscheidung>

Param4: Value = <Standardbegründung>

Param5: Value = <Nummer des Entscheidungsschritts> (PWODecisionStep.SubLevelNumber)

WhereClause: Value = "UID_AttestationCase ='"& $UID_AttestationCase$ &"'"
```

Durch die Parameter legen Sie fest, welcher Attestierungsvorgang durch die externe Entscheidung entschieden werden soll (`WhereClause`). Der Parameter `Param1` legt den Attestierer fest. Attestierer ist immer der Systembenutzer **sa**. Mit dem Parameter `Param2` wird die Entscheidung übergeben. Wurde der Attestierung zugestimmt, muss der Wert **True** übergeben werden. Wurde die Attestierung abgelehnt, muss der Wert **False** übergeben werden. Über den Parameter `Param3` übergeben Sie einen Begründungstext für die Entscheidung; über den Parameter `Param4` können Sie eine vorformulierte Standardbegründung übergeben. Wenn in einer Entscheidungsebene mehrere externe Entscheidungsschritte definiert wurden, übergeben Sie im Parameter `Param5` die Nummer des Entscheidungsschritts. Damit kann die Entscheidung dem korrekten Entscheidungsschritt zugeordnet werden.

Prozesse definieren und bearbeiten Sie mit dem Prozesseditor.

### Beispiel

Alle Complianceregeln sollen durch einen externen Gutachter geprüft und attestiert werden. Die Informationen über die Attestierungsobjekte sollen als PDF-Bericht auf einem externen Share bereitgestellt werden. Das Ergebnis der Attestierung soll der externe Gutachter in einer Textdatei auf dem externen Share ablegen. Nutzen Sie das Entscheidungsverfahren für extern vorzunehmende Entscheidungen und definieren Sie:

- einen Prozess "P1", der einen PDF-Report mit den Informationen über die Attestierungsobjekte und den Attestierungsvorgang auf einem externen Share ablegt
- ein Ereignis "E1", das den Prozess "P1" auslöst

  Das Ereignis "E1" tragen Sie im Entscheidungsschritt im Eingabefeld **Ereignis** und im Prozess "P1" als auslösendes Ereignis für die externe Entscheidung ein.
- einen Prozess "P2", der das externe Share auf neue Textdateien überprüft, den Inhalt der Textdatei auswertet und im One Identity Manager die Funktion `CallMethod` mit der Methode `MakeDecision` aufruft
- ein Ereignis "E2", das den Prozess "P2" auslöst
- einen Zeitplan, der regelmäßig das Ereignis "E2" auslöst

Ausführliche Informationen über die Erstellung von Prozessen finden Sie im *One Identity Manager Konfigurationshandbuch*. Ausführliche Informationen zur Einrichtung von Zeitplänen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.

### Detaillierte Informationen zum Thema

- Eigenschaften eines Entscheidungsschritts auf Seite 55

## Warten auf andere Entscheidung

HINWEIS: Pro Entscheidungsebene kann nur ein Entscheidungsschritt mit dem Entscheidungsverfahren WC definiert werden.

Wenn Sie sicherstellen wollen, dass ein definierter Datenzustand im One Identity Manager eingetreten ist, bevor ein Attestierungsvorgang endgültig entschieden wird, nutzen Sie das Entscheidungsverfahren WC. Durch eine Bedingung legen Sie fest, welche Voraussetzungen erfüllt sein müssen, damit eine Attestierung ausgeführt werden kann. Die Bedingung wird als Funktionsaufruf ausgewertet. Die Funktion muss als Parameter die UID des Attestierungsvorgangs (`AttestationCase.UID_AttestationCase`) akzeptieren. Über diese UID nehmen Sie auf das Attestierungsobjekt Bezug. Die Funktion muss drei Rückgabewerte als Integer-Werte definieren. Abhängig vom Rückgabewert der Funktion wird eine der folgenden Aktionen ausgeführt.

**Tabelle 24: Rückgabewerte für verzögerte Entscheidungen**

| Rückgabewert | Aktion |
|---|---|
| Rückgabewert > 0 | Die Bedingung ist erfüllt. Die verzögerte Entscheidung ist erfolgreich abgeschlossen. Der nächste Entscheidungsschritt (für den Erfolgsfall) wird ausgeführt. |
| Rückgabewert = 0 | Die Bedingung ist noch nicht erfüllt. Die Entscheidung wird zurückgestellt und beim nächsten Lauf des DBQueue Prozessors erneut geprüft. |
| Rückgabewert < 0 | Die Bedingung ist nicht erfüllt. Die verzögerte Entscheidung ist erfolglos abgeschlossen. Der nächste Entscheidungsschritt (für den Fehlerfall) wird ausgeführt. |

***Um das Entscheidungsverfahren nutzen zu können***

1. Erstellen Sie eine Datenbankfunktion, welche die Bedingung für die Attestierung prüft.
2. Erstellen Sie einen Entscheidungsschritt mit dem Entscheidungsverfahren WC. Erfassen Sie im Eingabefeld **Bedingung** den Funktionsaufruf.

   Syntax: `dbo.<Funktionsname>`
3. Legen Sie einen Entscheidungsschritt für den Erfolgsfall fest. Verwenden Sie ein Entscheidungsverfahren, mit dem der One Identity Manager die Attestierer ermitteln kann.
4. Legen Sie bei Bedarf einen Entscheidungsschritt für den Fehlerfall fest.

# Entscheidungsverfahren einrichten

Sollten die Standard-Entscheidungsverfahren zur Ermittlung der verantwortlichen Attestierer nicht Ihren Anforderungen entsprechen, können Sie eigene Entscheidungsverfahren erstellen. Die Bedingung, über die die Attestierer ermittelt werden, wird als Datenbankabfrage formuliert. Für eine Bedingung können mehrere Abfragen kombiniert werden.

***Um ein Entscheidungsverfahren einzurichten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsverfahren**.
2. Wählen Sie in der Ergebnisliste ein Entscheidungsverfahren und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

***Um die Bedingung zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsverfahren**.
2. Wählen Sie in der Ergebnisliste das Entscheidungsverfahren.
3. Wählen Sie die Aufgabe **Abfragen zur Ermittlung der Entscheider bearbeiten**.

### Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines Entscheidungsverfahrens auf Seite 81
- Abfragen zur Ermittlung der Attestierer auf Seite 82

## Allgemeine Stammdaten eines Entscheidungsverfahrens

Für ein Entscheidungsverfahren erfassen Sie folgende allgemeine Stammdaten.

**Tabelle 25: Allgemeine Stammdaten von Entscheidungsverfahren**

| Eigenschaft | Beschreibung |
|---|---|
| Entscheidungsverfahren | Kurzbezeichnung des Entscheidungsverfahrens (maximal zwei Zeichen). |
| Beschreibung | Bezeichnung des Entscheidungsverfahrens. |
| DBQueue Prozessor Aufgabe | Entscheidungen können entweder automatisch durch einen Berechnungsauftrag des DBQueue Prozessors getroffen werden oder durch festgelegte Attestierer. Wenn das Entscheidungsverfahren eine automatische Entscheidung treffen soll, weisen Sie eine kundendefinierte DBQueue Prozessor Aufgabe zu.<br>Wenn eine Abfrage zur Ermittlung der Attestierer erfasst ist, kann keine DBQueue Prozessor Aufgabe zugewiesen werden. |

| Eigenschaft | Beschreibung |
|---|---|
| Max. Anzahl Entscheider | Maximale Anzahl an Attestierern, die durch das Entscheidungsverfahren ermittelt werden. Wie viele Personen tatsächlich entscheiden müssen, legen Sie in den Entscheidungsschritten fest, die dieses Entscheidungsverfahren verwenden. |
| Reihenfolge | Wert für die Sortierung der Entscheidungsverfahren in Auswahllisten.<br>Um das Entscheidungsverfahren beim Einrichten eines Entscheidungsschrittes in der Auswahlliste an oberster Stelle anzuzeigen, legen Sie einen Wert kleiner '10' fest. |

### Verwandte Themen

- Eigenschaften eines Entscheidungsschritts auf Seite 55

## Abfragen zur Ermittlung der Attestierer

Die Bedingung, über die die Attestierer ermittelt werden, wird als Datenbankabfrage formuliert. Für eine Bedingung können mehrere Abfragen kombiniert werden. Dabei werden alle Personen in den Kreis der Attestierer aufgenommen, die durch die Einzelabfragen ermittelt werden.

***Um die Bedingung zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsverfahren**.
2. Wählen Sie in der Ergebnisliste das Entscheidungsverfahren.
3. Wählen Sie die Aufgabe **Abfragen zur Ermittlung der Entscheider bearbeiten**.

***Um eine einzelne Abfrage zu erstellen***

1. Klicken Sie **Hinzufügen**.

   Es wird eine neue Zeile in die Tabelle eingefügt.
2. Markieren Sie diese Zeile. Erfassen Sie die Eigenschaften der Abfrage.
3. Fügen Sie bei Bedarf weitere Abfragen hinzu.
4. Speichern Sie die Änderungen.

***Um eine einzelne Abfrage zu bearbeiten***

1. Wählen Sie in der Tabelle die Abfrage, die Sie bearbeiten möchten. Bearbeiten Sie die Eigenschaften der Abfrage.
2. Speichern Sie die Änderungen.

***Um eine einzelne Abfrage zu entfernen***

1. Wählen Sie in der Tabelle die Abfrage, die Sie entfernen möchten.
2. Klicken Sie **Entfernen**.
3. Speichern Sie die Änderungen.

**Tabelle 26: Eigenschaften einer Abfrage**

| Eigenschaft | Beschreibung |
|---|---|
| Entscheiderauswahl | Bezeichnung der Abfrage, die die Attestierer ermittelt. |
| Abfrage | Datenbankabfrage, die die Attestierer ermittelt.<br>Die Datenbankabfrage muss als Select-Anweisung formuliert werden. Die über die Datenbankabfrage ausgewählte Spalte muss eine `UID_Person` zurückgeben. Zusätzlich muss jede Abfrage einen Wert für `UID_PWORulerOrigin` übergeben. Ergebnis der Abfrage sind eine oder mehrere Personen, denen der Attestierungsvorgang zur Entscheidung vorgelegt wird. Liefert die Abfrage kein Ergebnis, wird das Attestierungsverfahren abgebrochen.<br>Eine Abfrage enthält genau eine Select-Anweisung. Um mehrere Select-Anweisungen zu kombinieren, erstellen Sie mehrere Abfragen.<br>Wenn eine DBQueue Prozessor Aufgabe zugewiesen ist, kann keine Abfrage zur Ermittlung der Attestierer erfasst werden. |

Die Abfrage kann beispielsweise vorher festgelegte Attestierer ermitteln (Beispiel 1). Die Attestierer können auch dynamisch in Abhängigkeit des Attestierungsvorgangs ermittelt werden. Dafür greifen Sie innerhalb der Datenbankabfrage über die Variable `@UID_AttestationCase` auf den Attestierungsvorgang zu (Beispiel 2).

## Beispiel 1

Die Attestierungsvorgänge sollen durch einen fest benannten Attestierer entschieden werden.

Abfrage:
```
select UID_Person, null as UID_PWORulerOrigin from Person where
InternalName='Bloggs, Jan'
```

## Beispiel 2

Alle aktiven Complianceregeln sollen durch die jeweiligen Regelverantwortlichen attestiert werden.

Abfrage:
```
select pia.UID_Person, null as UID_PWORulerOrigin from AttestationCase ac
    join ComplianceRule cr on cr.XObjectKey = ac.ObjectKeyBase and
    cr.IsWorkingCopy = '0'
    join PersonInBaseTree pia on pia.UID_Org = cr.UID_OrgResponsible and
    pia.XOrigin > 0
    where ac.UID_AttestationCase = @UID_AttestationCase
```

### Delegierungen berücksichtigen

Um bei der Ermittlung der Attestierer auch Delegierungen zu berücksichtigen, ermitteln Sie in der Abfrage auch die Personen, an die eine Verantwortlichkeit delegiert wurde. Wenn die Manager hierarchischer Rollen entscheiden sollen, ermitteln Sie die Attestierer aus der Tabelle HelperHeadOrg. Diese Tabelle vereinigt alle Manager von hierarchischen Rollen, deren Stellvertreter sowie die Personen, an die eine Verantwortlichkeit delegiert wurde. Wenn die Mitglieder von Geschäfts- oder Anwendungsrollen entscheiden sollen, ermitteln Sie die Entscheider aus der Tabelle PersonInBaseTree. Diese Tabelle vereinigt alle Mitglieder von hierarchischen Rollen sowie die Personen, an die eine Mitgliedschaft delegiert wurde.

Um den Delegierenden zu benachrichtigen, wenn der Empfänger der Delegierung einen Attestierungsvorgang entschieden hat, und damit im Web Portal angezeigt werden kann, ob der Attestierer aus einer Delegierung stammt, ermitteln Sie die UID_PWORulerOrigin.

#### *Um die UID_PWORulerOrigin der Delegierung zu ermitteln*

- Ermitteln Sie die UID_PersonWantsOrg der Delegierung und übernehmen Sie diesen Wert als UID_PWORulerOrigin in die Abfrage. Nutzen Sie dafür die Tabellenfunktion dbo.QER_FGIPWORulerOrigin.

  ```
  select dbo.QER_FGIPWORulerOrigin(XObjectKey) as UID_PWORulerOrigin
  ```

Angepasste Abfrage aus Beispiel 2:

```
select pia.UID_Person, dbo.QER_FGIPWORulerOrigin(pia.XObjectKey) as UID_
PWORulerOrigin from AttestationCase ac
    join ComplianceRule cr on cr.XObjectKey = ac.ObjectKeyBase and
    cr.IsWorkingCopy = '0'
    join PersonInBaseTree pia on pia.UID_Org = cr.UID_OrgResponsible and
    pia.XOrigin > 0
    where ac.UID_AttestationCase = @UID_AttestationCase
```

# Zusätzliche Aufgaben für Entscheidungsverfahren

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

# Überblick über das Entscheidungsverfahren

***Um einen Überblick über ein Entscheidungsverfahren zu erhalten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsverfahren**.
2. Wählen Sie in der Ergebnisliste das Entscheidungsverfahren.
3. Wählen Sie die Aufgabe **Überblick über das Entscheidungsverfahren**.

# Zulässige Entscheidungsverfahren für Tabellen festlegen

An Attestierungsverfahren können nur ausgewählte Entscheidungsrichtlinien zugewiesen werden. Welche Entscheidungsrichtlinien zugelassen sind, ist abhängig von den Entscheidungsverfahren, die in den Entscheidungsrichtlinien verwendet werden, und von der Tabelle, die das Basisobjekt der Attestierung für ein Attestierungsverfahren bildet. Für kundendefinierte Entscheidungsverfahren müssen Sie festlegen, mit welchen Tabellen diese Entscheidungsverfahren genutzt werden dürfen.

***Um festzulegen, für welche Tabellen ein Entscheidungsverfahren zulässig ist***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsverfahren**.
2. Wählen Sie in der Ergebnisliste das Entscheidungsverfahren.
3. Wählen Sie die Aufgabe **Tabellen zuweisen**.

   Weisen Sie im Bereich **Zuordnungen hinzufügen** die Tabellen zu, denen das Entscheidungsverfahren zugewiesen werden darf.

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

   ***Um eine Zuweisung zu entfernen***

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

Für welche Tabellen ein Entscheidungsverfahren zugelassen ist, sehen Sie auf dem Überblicksformular des Entscheidungsverfahrens.

## Verwandte Themen

- Entscheidungsrichtlinien zuweisen auf Seite 17
- Überblick über das Entscheidungsverfahren auf Seite 85

# Entscheidungsverfahren kopieren

Um beispielsweise Standard-Entscheidungsverfahren unternehmensspezifisch anzupassen, können Sie Entscheidungsverfahren kopieren und anschließend bearbeiten.

***Um ein Entscheidungsverfahren zu kopieren***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Entscheidungsverfahren**.
2. Wählen Sie in der Ergebnisliste ein Entscheidungsverfahren. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie die Aufgabe **Kopie erstellen**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Erfassen Sie die Kurzbezeichnung für die Kopie.

   Die Kurzbezeichnung eines Entscheidungsverfahrens besteht aus maximal zwei Zeichen.
6. Klicken Sie **Ok**, um die Kopieraktion zu starten.

   - ODER -

   Klicken Sie **Abbrechen**, um die Kopieraktion abzubrechen.

# Entscheidungsverfahren löschen

***Um ein Entscheidungsverfahren zu löschen***

1. Entfernen Sie alle Zuordnungen zu Entscheidungsschritten.
   a. Prüfen Sie auf dem Überblicksformular des Entscheidungsverfahrens, welchen Entscheidungsschritten das Entscheidungsverfahren zugeordnet ist.
   b. Wechseln Sie in den Entscheidungsworkflow und ordnen Sie dem Entscheidungsschritt ein anderes Entscheidungsverfahren zu.
2. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Kundendefiniert | Entscheidungsverfahren**.
3. Wählen Sie in der Ergebnisliste das Entscheidungsverfahren.
4. Klicken Sie .
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

## Verwandte Themen

- Überblick über das Entscheidungsverfahren auf Seite 85

# Ermitteln der verantwortlichen Attestierer

Welche Person in welcher Entscheidungsebene entscheidungsberechtigt ist, wird durch den DBQueue Prozessor berechnet. Sobald eine Attestierung ausgelöst wird, werden die Attestierer für alle Entscheidungsschritte des zu durchlaufenden Entscheidungsworkflows ermittelt. Änderungen in den Verantwortlichkeiten können dazu führen, dass eine Person für eine Attestierung, die noch nicht abschließend genehmigt ist, nun nicht mehr entscheidungsberechtigt ist. In diesem Fall müssen die Attestierer neu berechnet werden. Folgende Änderungen können eine Neuberechnung für noch nicht genehmigte Attestierungen auslösen:

- Entscheidungsrichtlinie, -workflow, -schritt oder -verfahren wurde geändert.
- Eine entscheidungsberechtigte Person verliert ihre Verantwortlichkeiten im One Identity Manager, beispielsweise wenn der Manager einer Abteilung, der Entscheider der Attestierungsrichtlinie oder der Zielsystemverantwortliche geändert wird.
- Eine Person erhält Verantwortlichkeiten im One Identity Manager und wird dadurch entscheidungsberechtigt, beispielsweise als Manager der zu attestierenden Person.
- Eine entscheidungsberechtigte Person wird deaktiviert.

Sobald für eine Person eine Verantwortlichkeit im One Identity Manager geändert wird, wird ein Auftrag zur Neuberechnung der Attestierer in die DBQueue eingestellt. Dabei werden standardmäßig alle Entscheidungsschritte der offenen Attestierungsvorgänge neu berechnet. Bereits genehmigte Entscheidungsschritte bleiben genehmigt, auch wenn sich deren Attestierer geändert hat. Abhängig von der Konfiguration der Systemumgebung und der Menge der zu verarbeitenden Daten kann die Neuberechnung der Attestierer viel Zeit beanspruchen. Um diese Verarbeitungszeit zu optimieren, können Sie festlegen, für welche Entscheidungsschritte die Attestierer neu berechnet werden sollen.

***Um die Neuberechnung der Attestierer zu konfigurieren***

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | ReducedApproverCalculation** und wählen Sie als Wert eine der folgenden Optionen.

**Tabelle 27: Optionen für die Neuberechnung von Attestierern**

| Option | Beschreibung |
|---|---|
| No | Alle Entscheidungsschritte werden neu berechnet. Dieses Verhalten gilt auch, wenn der Konfigurationsparameter deaktiviert ist.<br>Vorteil: Im Entscheidungsverlauf werden alle gültigen Attestierer angezeigt. Der weitere Entscheidungsverlauf ist transparent.<br>Nachteil: Die Neuberechnung der Attestierer kann viel Zeit beanspruchen. |
| CurrentLevel | Es werden nur die Attestierer für die aktuell zu bearbeitende Entscheidungsebene neu berechnet. Sobald eine Entscheidungsebene |

| Option | Beschreibung |
| --- | --- |
| | genehmigt wurde, werden die Attestierer für die folgende Entscheidungsebene aktuell ermittelt.<br><br>Vorteil: Die Anzahl der zu berechnenden Entscheidungsebenen wird reduziert. Die Berechnung der Attestierer wird möglicherweise beschleunigt.<br><br>TIPP: Nutzen Sie diese Option, wenn in Ihrer Umgebung Performance-Probleme im Zusammenhang mit der Neuberechnung der Attestierer auftreten.<br><br>Nachteil: Im Entscheidungsverlauf werden für jeden nachfolgenden Entscheidungsschritt noch die ursprünglich berechneten Attestierer angezeigt, die gegebenenfalls nicht mehr entscheidungsberechtigt sind. Die Darstellung des weiteren Entscheidungsverlaufs ist möglicherweise nicht korrekt. |
| NoRecalc | Keine Neuberechnung der Attestierer. Für die aktuelle Entscheidungsebene bleiben die bisherigen Attestierer entscheidungsberechtigt. Sobald eine Entscheidungsebene genehmigt wurde, werden die Attestierer für die folgende Entscheidungsebene aktuell ermittelt.<br><br>Vorteil: Die Anzahl der zu berechnenden Entscheidungsebenen wird reduziert. Die Berechnung der Attestierer wird möglicherweise beschleunigt.<br><br>TIPP: Nutzen Sie diese Option, wenn in Ihrer Umgebung Performance-Probleme im Zusammenhang mit der Neuberechnung der Attestierer auftreten, obwohl die Option **CurrentLevel** genutzt wird.<br><br>Nachteil: Im Entscheidungsverlauf werden für jeden nachfolgenden Entscheidungsschritt noch die ursprünglich berechneten Attestierer angezeigt, die gegebenenfalls nicht mehr entscheidungsberechtigt sind. Die Darstellung des weiteren Entscheidungsverlaufs ist möglicherweise nicht korrekt. Die aktuelle Entscheidungsebene können Personen entscheiden, die nicht mehr entscheidungsberechtigt sind.<br><br>Im ungünstigen Fall wurden hier ursprünglich nur Attestierer ermittelt, die nun keinen Zugang zum One Identity Manager haben, beispielsweise weil sie das Unternehmen verlassen haben. Die Entscheidungsebene kann nicht entschieden werden.<br><br>***Um solche Entscheidungsschritte dennoch abschließen zu können***<br><br>• Definieren Sie beim Einrichten der Entscheidungsworkflows an den Entscheidungsschritten ein Timeout und das Verhalten bei |

| Option | Beschreibung |
| --- | --- |
| | Timeout.<br>- ODER -<br>• Weisen Sie beim Einrichten der Attestierung Mitglieder an die zentrale Entscheidergruppe zu. Diese können jederzeit in offene Attestierungsvorgänge eingreifen. |

### Detaillierte Informationen zum Thema

- Eigenschaften eines Entscheidungsschritts auf Seite 55
- Zentrale Entscheidergruppe auf Seite 25

### Verwandte Themen

- Änderung des Entscheidungsworkflows bei offenen Attestierungsvorgängen auf Seite 106

# Einrichten der Multifaktor-Authentifizierung für Attestierungen

Für bestimmte sicherheitskritische Attestierungen kann eine zusätzliche Authentifizierung eingerichtet werden. Dabei muss jeder Attestierer bei der Attestierung einen Sicherheitscode eingeben. Welche Attestierungsrichtlinien diese Authentifizierung benötigen, legen Sie an der Attestierungsrichtlinien fest.

Für die Multifaktor-Authentifizierung nutzt der One Identity Manager One Identity Starling Two-Factor Authentication. Die benötigten Authentifizierungsinformationen sind in den Konfigurationsparametern unter **QER | Person | Starling** oder **QER | Person | Defender** festgelegt. Ausführliche Informationen zum Einrichten der Multifaktor-Authentifizierung finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

***Um die Multifaktor-Authentifizierung nutzen zu können***

1. Richten Sie die Multifaktor-Authentifizierung ein, wie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung* beschrieben.
2. Wählen Sie im Manager die Attestierungsrichtlinien, für welche die Multifaktor-Authentifizierung genutzt werden soll.
3. Aktivieren Sie die Option **Entscheidung durch Multifaktor Authentifizierung**.

   Für Standard-Attestierungsrichtlinien kann die Multifaktor-Authentifizierung nicht genutzt werden.

Sobald an einer Attestierungsrichtlinie die Option **Entscheidung durch Multifaktor Authentifizierung** aktiviert ist, wird in jedem Entscheidungsschritt des

Genehmigungsverfahrens ein Sicherheitscode angefordert. Das heißt, jede Person, die als Attestierer für diese Attestierungsrichtlinie ermittelt wird, muss ein Starling 2FA Token besitzen.

WICHTIG: Eine Attestierung per E-Mail ist nicht möglich, wenn für die Attestierungsrichtlinie die Multifaktor-Authentifizierung konfiguriert ist. Attestierungsmails für solche Attestierungen bewirken eine Fehlermeldung.

Ausführliche Informationen zur Multifaktor-Authentifizierung bei Attestierungen finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

### Verwandte Themen

- Allgemeine Stammdaten von Attestierungsrichtlinien auf Seite 28
- Attestierung per E-Mail auf Seite 122

# Attestierung durch die zu attestierende Person verhindern

In einem Attestierungsvorgang kann das Attestierungsobjekt gleichzeitig als Attestierer ermittelt werden. Damit können die zu attestierenden Personen sich selbst attestieren. Um das zu verhindern, aktivieren Sie den Konfigurationsparameter **QER | Attestation | PersonToAttestNoDecide**.

HINWEIS:

- Eine Änderung des Konfigurationsparameters wirkt nur auf neu zu erstellende Attestierungsvorgänge. Für bereits bestehende Attestierungsvorgänge werden die Attestierer nicht neu berechnet.
- Die Einstellung der Konfigurationsparameter gilt auch für Fallback-Entscheider; sie gilt nicht für die zentrale Entscheidergruppe.
- Wenn am Entscheidungsschritt die Option **Entscheidung durch betroffene Person** aktiviert ist, hat der Konfigurationsparameter keine Wirkung.

***Um zu verhindern, dass eine Person sich selbst attestieren darf***

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | PersonToAttestNoDecide**.

Der Konfigurationsparameter wirkt auf alle Attestierungsvorgänge, in denen Personen, die im Attestierungsobjekt oder in den Objektbeziehungen enthalten sind, gleichzeitig als Attestierer ermittelt werden. Folgende Personen werden aus dem Kreis der Attestierer entfernt:

- Personen, die in `AttestationCase.ObjectKeyBase` enthalten sind
- Personen, die in `AttestationCase.UID_ObjectKey1`, `ObjectKey2` oder `ObjectKey3`

enthalten sind

- die Hauptidentitäten dieser Personen
- alle Subidentitäten dieser Hauptidentitäten

Ist der Konfigurationsparameter nicht aktiviert oder ist am Entscheidungsschritt die Option **Entscheidung durch betroffene Person** aktiviert, dürfen diese Personen sich selbst attestieren.

### Verwandte Themen

Eigenschaften eines Entscheidungsschritts auf Seite 55

# Attestierungsvorgang steuern

Im Verlauf der Attestierung kann es notwendig sein, einen anderen als den standardmäßig verantwortlichen Attestierer mit der Attestierung zu beauftragen, beispielsweise weil ein verantwortlicher Attestierer abwesend ist. Möglicherweise werden zusätzliche Informationen über ein Attestierungsobjekt benötigt. Der One Identity Manager bietet verschiedene Möglichkeiten in einen offenen Attestierungsvorgang einzugreifen.

# Weitere Informationen einholen

Ein Attestierer hat die Möglichkeit weitere Informationen zu einem Attestierungsvorgang einzuholen. Diese Nachfragemöglichkeit ersetzt jedoch nicht die Genehmigung oder Ablehnung eines Attestierungsvorgangs. Zur Informationseinholung ist kein zusätzlicher Entscheidungsschritt in einem Entscheidungsworkflow erforderlich.

Der Attestierer kann eine Anfrage an jede beliebige Person stellen. Der Attestierungsvorgang erhält für den Zeitpunkt der Anfrage einen Hold-Status. Sobald die angefragte Person die benötigten Informationen geliefert hat und der Attestierer den Entscheidungsschritt entschieden hat, wird der Hold-Status wieder aufgehoben. Der Attestierer kann eine offene Anfrage jederzeit zurückrufen. Der Hold-Status wird dadurch aufgehoben. Die Anfrage und die Antwort werden im Entscheidungsverlauf aufgezeichnet und stehen somit den Attestierern zur Verfügung.

HINWEIS: Wenn der Attestierer, der eine Anfrage gestellt hat, als Entscheider entfällt, wird der Hold-Status aufgehoben. Die angefragte Person muss nicht mehr antworten. Der Attestierungsvorgang wird fortgesetzt.

Über offene Anfragen können E-Mail Benachrichtigungen an die beteiligten Personen versendet werden.

Ausführliche Informationen über Anfragen finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

### Detaillierte Informationen zum Thema

- E-Mail-Benachrichtigung: Benachrichtigungen bei Anfragen auf Seite 119

# Andere Attestierer beauftragen

Sobald eine Entscheidungsebene im Entscheidungsverlauf erreicht ist, können die Attestierer dieser Entscheidungsebene eine andere Person mit der Entscheidung beauftragen. Dafür stehen folgende Möglichkeiten zur Verfügung.

- Entscheidung umleiten

  Der Attestierer beauftragt eine andere Entscheidungsebene mit der Attestierung. Erstellen Sie dafür im Entscheidungsworkflow eine Verbindung zu der Entscheidungsebene, an die eine Entscheidung umgeleitet werden kann.

- Zusätzlichen Attestierer beauftragen

  Der Attestierer beauftragt eine weitere Person mit der Attestierung. Der weitere Attestierer muss zusätzlich zu den bereits ermittelten Attestierern entscheiden. Aktivieren Sie dafür am Entscheidungsschritt die Option **Zusätzliche Entscheider erlaubt**.

  Der zusätzliche Attestierer kann die Entscheidung verweigern und den Attestierungsvorgang an den ursprünglichen Attestierer zurückgeben. Der ursprüngliche Attestierer wird darüber per E-Mail informiert. Der ursprüngliche Attestierer kann einen anderen zusätzlichen Attestierer beauftragen.

- Entscheidung delegieren

  Der Attestierer beauftragt eine andere Person mit der Attestierung. Diese Person wird als Attestierer in den aktuellen Entscheidungsschritt aufgenommen. Sie entscheidet anstelle des delegierenden Attestierers. Aktivieren Sie dafür am Entscheidungsschritt die Option **Entscheidung delegierbar**.

  Der aktuelle Attestierer kann die Entscheidung verweigern und den Attestierungsvorgang an den ursprünglichen Attestierer zurückgeben. Der ursprüngliche Attestierer kann eine Delegierung zurücknehmen und an eine andere Person delegieren, beispielsweise wenn der andere Attestierer nicht verfügbar ist.

Es können E-Mail Benachrichtigungen an die anderen und die ursprünglichen Attestierer versendet werden.

### Detaillierte Informationen zum Thema

- Entscheidungsebenen verbinden auf Seite 60
- Entscheidungsebenen bearbeiten auf Seite 54
- Eigenschaften eines Entscheidungsschritts auf Seite 55

### Verwandte Themen

- E-Mail-Benachrichtigung: Delegierung von Attestierungen auf Seite 118
- E-Mail-Benachrichtigung: Zurückweisen von Entscheidungen auf Seite 119
- E-Mail-Benachrichtigung: Benachrichtigungen von zusätzlichen Attestierern auf Seite 120

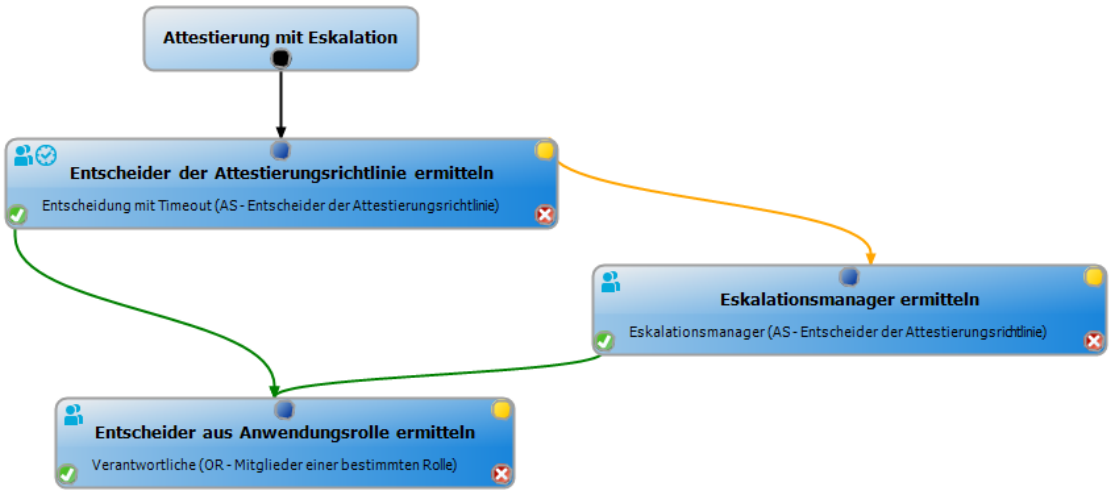
# Eskalieren eines Attestierungsvorgangs

Entscheidungsschritte können bei Überschreitung eines festgelegten Zeitraumes automatisch eskaliert werden. Der Attestierungsvorgang wird einem weiteren Entscheiderkreis vorgelegt. Anschließend wird der Attestierungsvorgang wieder im normalen Entscheidungsworkflow weiter bearbeitet.

***Um die Eskalation eines Entscheidungsschrittes zu konfigurieren***

1. Öffnen Sie den Entscheidungsworkflow im Workfloweditor.
2. Fügen Sie eine zusätzliche Entscheidungsebene mit einem Entscheidungsschritt zur Eskalation ein.
3. Verbinden Sie den Entscheidungsschritt, der bei Zeitüberschreitung eskaliert werden soll, mit dem neuen Entscheidungsschritt. Nutzen Sie dazu den Verbindungspunkt für Eskalation.

**Abbildung 3: Beispiel für einen Entscheidungsworkflow mit Eskalation**




4. Konfigurieren Sie am Entscheidungsschritt, der bei Zeitüberschreitung eskaliert werden soll, das Verhalten.

**Tabelle 28: Eigenschaften für die Eskalation bei Zeitüberschreitung**

| Eigenschaft | Bedeutung |
|---|---|
| Timeout (Arbeitsstunden) | Anzahl der Arbeitsstunden, nach deren Ablauf der Entscheidungsschritt automatisch entschieden wird.<br>Das Timeout wird standardmäßig alle 30 Minuten geprüft. Um das Prüfintervall zu ändern, passen Sie den Zeitplan **Erinnerungsintervall und Timeout von Attestierungsvorgängen prüfen** an.<br>Für die Zeitberechnung wird die gültige Arbeitszeit des jeweiligen Entscheiders berücksichtigt.<br>HINWEIS: Für die Ermittlung der gültigen Arbeitszeiten stellen Sie sicher, dass in den Stammdaten der Personen ein Bundesland und/oder ein Bundesstaat eingetragen ist. Wenn diese Informationen fehlen, wird ein Fallback zur Berechnung der Arbeitszeit genutzt. Ausführliche Informationen zur Ermittlung der Arbeitszeit von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.<br>Wurden mehrere Entscheider ermittelt, dann wird der Entscheidungsschritt erst dann automatisch entschieden, wenn der Timeout für alle Entscheider überschritten ist. Gleiches gilt, wenn ein zusätzlicher Entscheider beauftragt wurde.<br>Hat ein Entscheider die Entscheidung delegiert, wird der Zeitpunkt für die automatische Entscheidung für den neuen Entscheider neu berechnet. Wenn dieser die Entscheidung zurückweist, wird der Zeitpunkt für die automatische Entscheidung für den ursprünglichen Entscheider neu berechnet.<br>Wenn ein Entscheider eine Anfrage stellt, muss die Entscheidung trotzdem innerhalb des definierten Timeouts getroffen werden. Der Zeitpunkt für die automatische Entscheidung wird nicht neu berechnet. |
| Verhalten bei Timeout | Aktion, die im Falle einer Zeitüberschreitung ausgeführt wird.<br>• **Eskalation**: Der Attestierungsvorgang wird eskaliert. Es wird die Entscheidungsebene zur Eskalation aufgerufen. |

Bei einer Eskalation können E-Mail-Benachrichtigungen an die neuen Attestierer und weitere Personen versendet werden.

## Verwandte Themen

- E-Mail-Benachrichtigung: Aufforderung zur Attestierung
- E-Mail-Benachrichtigung: Eskalation von Attestierungsvorgängen auf Seite 118

# Attestierer können nicht ermittelt werden

Für den Fall, dass Attestierungsvorgänge nicht entschieden werden können, weil kein Attestierer verfügbar ist, können Sie Fallback-Entscheider festlegen. Ein Attestierungsvorgang wird immer dann an die Fallback-Entscheider zur Attestierung zugewiesen, wenn in einem Entscheidungsschritt über das festgelegte Entscheidungsverfahren kein Attestierer ermittelt werden kann.

Um Fallback-Entscheider festzulegen, definieren Sie Anwendungsrollen und weisen diese den Entscheidungsschritten zu. Unterschiedliche Attestiererkreise in den Entscheidungsschritten erfordern gegebenenfalls auch unterschiedliche Fallback-Entscheider. Legen Sie dafür verschiedene Anwendungsrollen an, denen Sie die Personen zuweisen, die als Fallback-Entscheider in den Genehmigungsverfahren ermittelt werden sollen. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

### *Um Fallback-Entscheider für einen Entscheidungsschritt festzulegen*

- Erfassen Sie am Entscheidungsschritt die folgenden Daten.

**Tabelle 29: Eigenschaften des Entscheidungsschritts für Fallback-Entscheider**

| Eigenschaft | Bedeutung |
|---|---|
| Fallback-Entscheider | Anwendungsrolle, deren Mitglieder berechtigt sind, die Attestierungsvorgänge zu entscheiden, wenn durch das Entscheidungsverfahren kein Attestierer ermittelt werden kann. Weisen Sie eine Anwendungsrolle aus der Auswahlliste zu.<br>Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.<br>HINWEIS: Die Anzahl der Entscheider wird nicht auf die Fallback-Entscheider angewendet. Der Entscheidungsschritt gilt als entschieden, sobald 1 Fallback-Entscheider entschieden hat. |

### *Ablauf einer Attestierung mit Fallback-Entscheider*

1. In einem Genehmigungsverfahren kann für einen Entscheidungsschritt kein Attestierer ermittelt werden. Der Attestierungsvorgang wird allen Mitgliedern der Anwendungsrolle für Fallback-Entscheider zugewiesen.
2. Sobald ein Fallback-Entscheider den Attestierungsvorgang genehmigt hat, wird der Attestierungsvorgang den Attestierern der nächsten Entscheidungsebene vorgelegt.

HINWEIS: Am Entscheidungsschritt kann festgelegt werden, wie viele Attestierer diesen Entscheidungsschritt entscheiden müssen. Diese Beschränkung gilt **nicht** für die Fallback-Entscheider. Der Entscheidungsschritt gilt als entschieden, sobald **ein** Fallback-Entscheider die Attestierung entschieden hat.

3. Wenn kein Fallback-Entscheider ermittelt werden kann, wird der Attestierungsvorgang abgebrochen.

Fallback-Entscheider können Attestierungsvorgänge für alle manuellen Entscheidungsschritte entscheiden. Für Entscheidungsschritte mit den Entscheidungsverfahren CD, EX und WC sind keine Fallback-Entscheidungen möglich.

### Verwandte Themen

- Entscheidungsebenen bearbeiten auf Seite 54
- Auswahl der verantwortlichen Attestierer auf Seite 62
- Attestierungen durch die zentrale Entscheidergruppe auf Seite 100

# Automatische Entscheidung bei Zeitüberschreitung

Attestierungsvorgänge können bei Überschreitung eines festgelegten Zeitraumes automatisch entschieden werden.

***Um die automatische Entscheidung nach Zeitüberschreitung zu konfigurieren***

- Erfassen Sie am Entscheidungsschritt die folgenden Daten.

**Tabelle 30: Eigenschaften für die automatische Entscheidung bei Zeitüberschreitung**

| Eigenschaft | Bedeutung |
|---|---|
| Timeout (Arbeitsstunden) | Anzahl der Arbeitsstunden, nach deren Ablauf der Entscheidungsschritt automatisch entschieden wird.<br>Das Timeout wird standardmäßig alle 30 Minuten geprüft. Um das Prüfintervall zu ändern, passen Sie den Zeitplan **Erinnerungsintervall und Timeout von Attestierungsvorgängen prüfen** an.<br>Für die Zeitberechnung wird die gültige Arbeitszeit des jeweiligen Entscheiders berücksichtigt.<br>HINWEIS: Für die Ermittlung der gültigen Arbeitszeiten stellen Sie sicher, dass in den Stammdaten der Personen ein Bundesland und/oder ein Bundesstaat eingetragen ist. Wenn diese Informationen fehlen, wird ein Fallback zur Berechnung der Arbeitszeit genutzt. Ausführliche Informationen zur Ermittlung der Arbeitszeit von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.<br>Wurden mehrere Entscheider ermittelt, dann wird der Entscheidungsschritt erst dann automatisch entschieden, wenn der Timeout für alle Entscheider überschritten ist. Gleiches gilt, wenn ein zusätzlicher Entscheider beauftragt wurde.<br>Hat ein Entscheider die Entscheidung delegiert, wird der Zeitpunkt für die automatische Entscheidung für den neuen Entscheider neu berechnet. Wenn dieser die Entscheidung zurückweist, wird der Zeitpunkt für die automatische Entscheidung für den ursprünglichen Entscheider neu berechnet.<br>Wenn ein Entscheider eine Anfrage stellt, muss die Entscheidung trotzdem innerhalb des definierten Timeouts getroffen werden. Der Zeitpunkt für die automatische Entscheidung wird nicht neu berechnet. |
| Verhalten bei Timeout | Aktion, die im Falle einer Zeitüberschreitung ausgeführt wird.<br>• **Genehmigung**: Der Attestierungsvorgang wird in diesem Entscheidungsschritt genehmigt. Es wird die nächste Entscheidungsebene aufgerufen.<br>• **Ablehnung**: Der Attestierungsvorgang wird in diesem Entscheidungsschritt abgelehnt. Es wird die Entscheidungsebene für Ablehnung aufgerufen. |

Bei der automatischen Entscheidung eines Attestierungsvorgangs kann eine E-Mail Benachrichtigung an weitere Personen versendet werden.

### Verwandte Themen

- E-Mail-Benachrichtigung: Genehmigung oder Ablehnung von Attestierungsvorgängen auf Seite 115
- Entscheidungsebenen bearbeiten auf Seite 54

# Abbruch eines Attestierungsvorgangs bei Zeitüberschreitung

Attestierungsvorgänge können bei Überschreitung eines festgelegten Zeitraumes automatisch abgebrochen werden. Der Abbruch kann erfolgen, wenn ein einzelner Entscheidungsschritt oder das gesamte Genehmigungsverfahren einen bestimmten Zeitraum überschreitet.

***Um den Abbruch nach Zeitüberschreitung eines einzelnen Entscheidungsschrittes zu konfigurieren***

- Erfassen Sie am Entscheidungsschritt die folgenden Daten.

**Tabelle 31: Eigenschaften des Entscheidungsschritts für den Abbruch bei Zeitüberschreitung**

| Eigenschaft | Bedeutung |
|---|---|
| Timeout (Arbeitsstunden) | Anzahl der Arbeitsstunden, nach deren Ablauf der Entscheidungsschritt automatisch entschieden wird.<br><br>Das Timeout wird standardmäßig alle 30 Minuten geprüft. Um das Prüfintervall zu ändern, passen Sie den Zeitplan **Erinnerungsintervall und Timeout von Attestierungsvorgängen prüfen** an.<br><br>Für die Zeitberechnung wird die gültige Arbeitszeit des jeweiligen Entscheiders berücksichtigt.<br><br>HINWEIS: Für die Ermittlung der gültigen Arbeitszeiten stellen Sie sicher, dass in den Stammdaten der Personen ein Bundesland und/oder ein Bundesstaat eingetragen ist. Wenn diese Informationen fehlen, wird ein Fallback zur Berechnung der Arbeitszeit genutzt. Ausführliche Informationen zur Ermittlung der Arbeitszeit von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.<br><br>Wurden mehrere Entscheider ermittelt, dann wird der Entscheidungsschritt erst dann automatisch entschieden, wenn der Timeout für alle Entscheider überschritten ist. Gleiches gilt, wenn ein zusätzlicher Entscheider beauftragt wurde.<br><br>Hat ein Entscheider die Entscheidung delegiert, wird der Zeitpunkt für die automatische Entscheidung für den neuen Entscheider neu berechnet. Wenn dieser die Entscheidung zurückweist, wird der Zeitpunkt für die automatische Entscheidung für den ursprünglichen Entscheider neu berechnet.<br><br>Wenn ein Entscheider eine Anfrage stellt, muss die Entscheidung trotzdem innerhalb des definierten Timeouts getroffen werden. Der Zeitpunkt für die automatische Entscheidung wird nicht neu berechnet. |
| Verhalten bei Timeout | Aktion, die im Falle einer Zeitüberschreitung ausgeführt wird.<br><br>• **Abbruch**: Der Entscheidungsschritt, und somit das gesamte Attestierungsverfahren, wird abgebrochen. |

***Um den Abbruch nach Zeitüberschreitung des gesamten Genehmigungsverfahrens zu konfigurieren***

- Erfassen Sie am Entscheidungsworkflow die folgenden Daten.

**Tabelle 32: Eigenschaften des Entscheidungsworkflows für den Abbruch bei Zeitüberschreitung**

| Eigenschaft | Bedeutung |
|---|---|
| Systemabbruch (Tage) | Anzahl der Tage, nach deren Ablauf der Entscheidungsworkflow, und somit das gesamte Attestierungsverfahren, automatisch durch das System beendet wird. |

Bei Abbruch eines Attestierungsvorgangs kann eine E-Mail Benachrichtigung an weitere Personen versendet werden.

### Verwandte Themen

- E-Mail-Benachrichtigung: Abbruch von Attestierungsvorgängen
- Entscheidungsebenen bearbeiten auf Seite 54
- Entscheidungsworkflows einrichten auf Seite 53

# Attestierungen durch die zentrale Entscheidergruppe

Mitunter können Attestierungsvorgänge nicht entschieden werden, da ein Attestierer nicht verfügbar ist oder keinen Zugang zu den One Identity Manager Werkzeugen hat. Um solche Attestierungsvorgänge dennoch abzuschließen, können Sie eine zentrale Entscheidergruppe festlegen, deren Mitglieder berechtigt sind, zu jedem Zeitpunkt in die Genehmigungsverfahren einzugreifen.

Die zentralen Entscheider sind berechtigt in besonderen Fällen Attestierungen zu genehmigen, abzulehnen, abzubrechen oder andere Attestierer zu beauftragen.

WICHTIG:

- Da die zentralen Entscheider Attestierungsvorgänge jederzeit entscheiden können, kann mit deren Entscheidungen das 4-Augen-Prinzip für Genehmigungen durchbrochen werden. Legen Sie unternehmensspezifisch fest, in welchen besonderen Fällen die zentrale Entscheidergruppe in Genehmigungsverfahren eingreifen darf.
- Zentrale Entscheider dürfen sich selbst attestieren. Die Einstellung des Konfigurationsparameters **QER | Attestation | PersonToAttestNoDecide** gilt nicht für die zentrale Entscheidergruppe.
- Am Entscheidungsschritt kann festgelegt werden, wie viele Attestierer diesen Entscheidungsschritt entscheiden müssen. Diese Beschränkung gilt nicht für die zentrale Entscheidergruppe. Der Entscheidungsschritt gilt als entschieden, sobald 1 Mitglied aus der zentralen Entscheidergruppe die Attestierung entschieden hat.

Die zentrale Entscheidergruppe kann Attestierungen für alle manuellen Entscheidungsschritte entscheiden. Dabei gilt:

- Für Entscheidungsschritte mit den Entscheidungsverfahren CD, EX und WC sind keine zentralen Entscheidungen möglich.
- Wenn ein Mitglied der zentralen Entscheidergruppe für einen Entscheidungsschritt auch als regulärer Attestierer ermittelt wird, dann kann er diesen Entscheidungsschritt nur als regulärer Attestierer entscheiden.
- Die zentrale Entscheidergruppe kann auch entscheiden, wenn ein regulärer Attestierer eine Anfrage gestellt hat und sich der Attestierungsvorgang im Hold-Status befindet.

***Um Mitglieder in die zentrale Entscheidergruppe aufzunehmen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Basisdaten zur Konfiguration | Zentrale Entscheidergruppe**.
2. Wählen Sie die Aufgabe **Personen zuweisen**.

   Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu, die berechtigt sind alle Attestierungen zu entscheiden.

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

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Person und doppelklicken Sie ✓.
3. Speichern Sie die Änderungen.

## Verwandte Themen

- Zentrale Entscheidergruppe auf Seite 25

# 3

# Ablauf einer Attestierung

Sobald eine Attestierung automatisch oder manuell angestoßen wird, erstellt der One Identity Manager für jedes Attestierungsobjekt einen Attestierungsvorgang. Attestierungsvorgänge zeichnen den gesamten Ablauf einer Attestierung auf. Im Attestierungsvorgang kann jeder einzelne Entscheidungsschritt der Attestierung revisionssicher nachvollzogen werden.

Attestierungsvorgänge sehen Sie in der Navigationsansicht unter dem Menüeintrag **Attestierungsläufe | <Attestierungsrichtlinie>**. Hier können Sie den Status der Attestierungsvorgänge überwachen. Attestierungsvorgänge, die noch nicht entschieden wurden, werden unter dem Filter **Offene Attestierungen** angezeigt. Unter dem Filter **Abgeschlossene Attestierungen** sehen Sie Attestierungsvorgänge, die durch die Attestierer oder durch den One Identity Manager abgeschlossen wurden.

HINWEIS: Attestierungsvorgänge werden im Web Portal bearbeitet. Ausführliche Informationen dazu finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

Mit der Genehmigung oder Ablehnung eines Attestierungsvorgangs ist die Attestierung abgeschlossen. Wie mit abgelehnten oder genehmigten Attestierungen weiter verfahren werden soll, legen Sie unternehmensspezifisch fest.

TIPP: Der One Identity Manager stellt für verschiedene Datensituationen Standard-Attestierungsverfahren und Standard-Attestierungsrichtlinien bereit. Wenn Sie diese Standard-Attestierungsverfahren nutzen, können Sie konfigurieren, wie mit abgelehnten Attestierungen weiter verfahren werden soll.

Weitere Informationen finden Sie unter Standardattestierungen und der Entzug von Berechtigungen auf Seite 126.

## Attestierung starten

Um Attestierungsvorgänge anzulegen, stehen Ihnen im One Identity Manager zwei Möglichkeiten zur Verfügung. Sie können Attestierungen durch einen zeitgesteuerten Auftrag auslösen oder für ausgewählte Objekte einzeln starten.

***Voraussetzung***

- Die Attestierungsrichtlinie, für die Attestierungen durchgeführt werden sollen, ist aktiviert.

***Um Attestierungen über einen zeitgesteuerten Auftrag zu starten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Aktivieren Sie den Zeitplan, der im Eingabefeld **Zeitplan der Berechnung** eingetragen ist.
    a. Wählen Sie in der Navigationsansicht **Basisdaten zur Konfiguration | Zeitpläne**.
    b. Wählen Sie in der Ergebnisliste den Zeitplan und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
    c. Aktivieren Sie die Option **Aktiviert**.
    d. Speichern Sie die Änderungen.

***Um Attestierungen für ausgewählte Objekte zu starten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie die Aufgabe **Attestierungsvorgänge für einzelne Objekte jetzt erstellen**.

    Ein separates Fenster wird geöffnet.
4. Aktivieren Sie in der Spalte **Attestierung** jedes Objekt, für das die Attestierung durchgeführt werden soll.
5. Klicken Sie **Starten**.

    Für die ausgewählten Attestierungsobjekte werden Attestierungsvorgänge erstellt. Sobald der DBQueue Prozessor den Auftrag bearbeitet hat, sehen Sie die neu erstellten Attestierungsvorgänge in der Navigationsansicht unter dem Menüeintrag **Attestierungsläufe | <Attestierungsrichtlinie> | Attestierungsläufe | <Jahr> | <Monat> | <Tag> | Offene Attestierungen**.
6. Klicken Sie **Schließen**.

HINWEIS: Unter bestimmten Voraussetzungen werden beim Anlegen neuer Attestierungsvorgänge alte, abgeschlossene Attestierungsvorgänge aus der One Identity Manager-Datenbank gelöscht.

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

### Detaillierte Informationen zum Thema

- Allgemeine Stammdaten von Attestierungsrichtlinien auf Seite 28
- Zeitpläne auf Seite 19

### Verwandte Themen

- Attestierung für einzelne Objekte starten auf Seite 35
- Ermitteln der verantwortlichen Attestierer auf Seite 87
- Attestierungsvorgänge löschen auf Seite 108

# Zusätzliche Aufgaben für Attestierungsvorgänge

Sobald die Attestierung für eine Attestierungsrichtlinie gestartet wurde, können Sie den Status des Attestierungsvorgangs im One Identity Manager überwachen. In der Aufgabenansicht eines Attestierungsvorgangs stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können.

## Überblick über Attestierungsvorgänge

Über das Überblicksformular erhalten Sie die wichtigsten Informationen zum Attestierungsvorgang. Abhängig von der Bearbeitungszeit sehen Sie hier, bis wann ein Attestierungsvorgang bearbeitet werden soll. Der One Identity Manager gibt nicht vor, welche Aktionen ausgeführt werden, wenn die Bearbeitungszeit überschritten ist. Definieren Sie für diesen Fall unternehmensspezifische Aktionen oder Auswertungen.

***Um einen Überblick über einen Attestierungsvorgang zu erhalten***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsläufe | <Attestierungsrichtlinie> | Attestierungsläufe | <Jahr> | <Monat> | <Tag>**.
2. Wählen Sie den Filter **Offene Attestierungen** oder **Abgeschlossene Attestierungen**.
3. Wählen Sie in der Ergebnisliste den Attestierungsvorgang.
4. Wählen Sie die Aufgabe **Überblick über den Attestierungsvorgang**.

# Entscheidungsverlauf

Für offene Attestierungsvorgänge sehen Sie den aktuellen Stand des Genehmigungsverfahrens. Der Entscheidungsverlauf wird angezeigt, sobald der DBQueue Prozessor die Attestierer für den ersten Entscheidungsschritt ermittelt hat. Im Entscheidungsverlauf sehen Sie den Entscheidungsworkflow, die Ergebnisse der einzelnen Entscheidungsschritte und die ermittelten Attestierer. Konnte das Entscheidungsverfahren keinen Attestierer ermitteln, wird der Attestierungsvorgang durch das System abgebrochen.

***Um den Entscheidungsverlauf eines offenen Attestierungsvorgangs anzuzeigen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsläufe | <Attestierungsrichtlinie> | Attestierungsläufe | <Jahr> | <Monat> | <Tag> | Offene Attestierungen**.
2. Wählen Sie in der Ergebnisliste den Attestierungsvorgang.
3. Wählen Sie die Aufgabe **Entscheidungsverlauf**.

Die einzelnen Entscheidungsebenen eines Entscheidungsworkflows werden über ein spezielles Steuerelement dargestellt. Die verantwortlichen Attestierer eines Entscheidungsschrittes werden über einen Tooltip angezeigt. Offene Nachfragen zu einem Entscheidungsschritt werden ebenfalls im Tooltip angezeigt. Die Steuerelemente werden farblich hinterlegt. Der Farbcode spiegelt den aktuellen Status der Entscheidungsebenen wieder.

**Tabelle 33: Bedeutung der Farben im Entscheidungsverlauf (in absteigender Priorität)**

| Farbe | Bedeutung |
|---|---|
| Blau | Die Entscheidungsebene wird aktuell bearbeitet. |
| Grün | Die Entscheidungsebene wurde positiv entschieden. |
| Rot | Die Entscheidungsebene wurde negativ entschieden. |
| Gelb | Die Entscheidungsebene wurde aufgrund einer Nachfrage zurückgestellt. |
| Grau | Die Entscheidungsebene wurde (noch) nicht erreicht. |

# Attestierungshistorie

In der Attestierungshistorie werden die einzelnen Schritte des Attestierungsvorgangs dargestellt. Sie können hier den zeitlichen Ablauf und die Entscheidungen im Genehmigungsverfahren nachvollziehen. Die Attestierungshistorie wird sowohl für offene als auch für abgeschlossene Attestierungen angezeigt.

***Um die Attestierungshistorie eines Attestierungsvorgangs anzuzeigen***

1. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsläufe | <Attestierungsrichtlinie> | Attestierungsläufe | <Jahr> | <Monat> | <Tag>**.
2. Wählen Sie den Filter **Offene Attestierungen** oder **Abgeschlossene Attestierungen**.
3. Wählen Sie in der Ergebnisliste den Attestierungsvorgang.
4. Wählen Sie den Bericht **Attestierungshistorie**.

Die Steuerelemente werden farblich hinterlegt. Der Farbcode spiegelt den Status der Entscheidungsschritte wieder.

**Tabelle 34: Bedeutung der Farben in der Attestierungshistorie**

| Farbe | Bedeutung |
|---|---|
| Gelb | Attestierungsvorgang erstellt. |
| Grün | Attestierer hat genehmigt. |
| Rot | Attestierer hat abgelehnt.<br>Attestierung wurde eskaliert.<br>Attestierer hat seine Entscheidung widerrufen. |
| Grau | Attestierung wurde abgebrochen.<br>Vorgang wurde an einen zusätzlichen Attestierer zugewiesen.<br>Zusätzlicher Attestierer hat die Entscheidung zurückgewiesen.<br>Entscheidung wurde delegiert.<br>Neuer Attestierer hat die Delegierung zurückgewiesen. |
| Orange | Attestierer hat eine Nachfrage.<br>Nachfrage wurde beantwortet.<br>Nachfrage wurde wegen Entscheiderwechsel abgebrochen. |
| Blau | Attestierer hat die Entscheidung umgeleitet.<br>Der Entscheidungsschritt wurde automatisch zurückgesetzt. |

# Änderung des Entscheidungsworkflows bei offenen Attestierungsvorgängen

Wenn Entscheidungsworkflows geändert werden, muss entschieden werden, ob diese Änderungen auf offene Attestierungsvorgänge übernommen werden sollen. Das gewünschte Vorgehen wird über Konfigurationsparameter festgelegt.

## Szenario: An der Entscheidungsrichtlinie wurde ein anderer Entscheidungsworkflow hinterlegt

Wenn in einer Entscheidungsrichtlinie der Entscheidungsworkflow geändert wurde, werden offene Genehmigungsverfahren standardmäßig mit dem ursprünglichen Workflow fortgesetzt. Der neu hinterlegte Workflow wird nur in neuen Attestierungsvorgängen genutzt. Ein abweichendes Verhalten kann konfiguriert werden.

***Um festzulegen, wie mit offenen Attestierungsvorgängen verfahren werden soll***

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | OnWorkflowAssign** und wählen Sie einen der folgenden Werte.
  - **CONTINUE**: Laufende Genehmigungsverfahren werden mit dem ursprünglich gültigen Workflow fortgesetzt. Der neu hinterlegte Workflow wird nur in neuen Attestierungsvorgängen genutzt.

    Dieses Verhalten gilt auch, wenn der Konfigurationsparameter deaktiviert ist.
  - **RESET**: In laufenden Genehmigungsverfahren werden alle bereits getroffenen Entscheidungen zurückgesetzt. Die Genehmigungsverfahren werden mit dem neu hinterlegten Workflow erneut gestartet. Die Attestierungsvorgänge durchlaufen das Genehmigungsverfahren erneut.
  - **ABORT**: Laufende Genehmigungsverfahren werden abgebrochen. Alle offenen Attestierungsvorgänge werden geschlossen. Beim nächsten automatischen oder manuellen Start der Attestierung wird der neue Entscheidungsworkflow genutzt.

Es wird eine Arbeitskopie des ursprünglich gültigen Workflows gespeichert. Die Arbeitskopie bleibt erhalten, solange sie noch in laufenden Genehmigungsverfahren genutzt wird. Alle ungenutzten Arbeitskopien werden über den Zeitplan **Wartung Entscheidungsworkflows** regelmäßig gelöscht.

## Szenario: Ein genutzter Entscheidungsworkflow wurde geändert

Wenn ein Entscheidungsworkflow geändert wurde, der in offenen Attestierungsvorgängen genutzt wird, werden die offenen Genehmigungsverfahren standardmäßig mit dem ursprünglichen Workflow fortgesetzt. Die Änderungen am Entscheidungsworkflow sind nur für neue Attestierungsvorgänge wirksam. Ein abweichendes Verhalten kann konfiguriert werden.

***Um festzulegen, wie mit offenen Attestierungsvorgängen verfahren werden soll***

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | OnWorkflowUpdate** und wählen Sie einen der folgenden Werte.
  - **CONTINUE**: Laufende Genehmigungsverfahren werden mit dem ursprünglich gültigen Entscheidungsworkflow fortgesetzt. Die Änderungen am Entscheidungsworkflow sind nur für neue Attestierungsvorgänge wirksam.

    Dieses Verhalten gilt auch, wenn der Konfigurationsparameter deaktiviert ist.
  - **RESET**: In laufenden Genehmigungsverfahren werden alle bereits getroffenen

Entscheidungen zurückgesetzt. Die Genehmigungsverfahren werden mit dem geänderten Entscheidungsworkflow erneut gestartet. Die Attestierungsvorgänge durchlaufen das Genehmigungsverfahren erneut.

- **ABORT**: Laufende Genehmigungsverfahren werden abgebrochen. Alle offenen Attestierungsvorgänge werden geschlossen. Beim nächsten automatischen oder manuellen Start der Attestierung wird der geänderte Entscheidungsworkflow genutzt.

Es wird eine Arbeitskopie des Entscheidungsworkflows gespeichert, welche die ursprüngliche Version enthält. Diese Arbeitskopie bleibt erhalten, solange sie noch in laufenden Genehmigungsverfahren genutzt wird. Alle ungenutzten Arbeitskopien werden über den Zeitplan **Wartung Entscheidungsworkflows** regelmäßig gelöscht.

### Verwandte Themen

- Ermitteln der verantwortlichen Attestierer auf Seite 87

# Attestierungsvorgänge für deaktivierte Personen schließen

Offene Attestierungsvorgänge müssen auch dann noch bearbeitet werden, wenn die zu attestierende Person zwischenzeitlich dauerhaft deaktiviert wurde. Häufig ist das nicht nötig, da die betroffene Person beispielsweise das Unternehmen verlassen hat. Dafür gibt es die Möglichkeit die offenen Attestierungsvorgänge einer Person automatisch zu schließen, wenn diese Person dauerhaft deaktiviert wird.

***Um Attestierungsvorgänge automatisiert zu schließen***

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | AutoCloseInactivePerson**.

Der Konfigurationsparameter wirkt, wenn die zu attestierende Person erst deaktiviert wird, nachdem der Attestierungsvorgang erstellt wurde.

Der Konfigurationsparameter wirkt nicht, wenn die Person zeitweilig deaktiviert wird.

TIPP: Damit für deaktivierte Personen keine Attestierungsvorgänge erstellt werden, formulieren Sie die Bedingung zur Ermittlung der Attestierungsobjekte an den Attestierungsrichtlinien entsprechend. Weitere Informationen finden Sie unter Allgemeine Stammdaten von Attestierungsrichtlinien auf Seite 28.

# Attestierungsvorgänge löschen

Wenn regelmäßig Attestierungen durchgeführt werden, wächst die Tabelle `AttestationCase` sehr schnell. Um die Zahl der Attestierungsvorgänge in der One Identity Manager-

Datenbank zu beschränken, können Sie veraltete, abgeschlossene Attestierungsvorgänge aus der Datenbank entfernen. Dabei werden die Eigenschaften der Attestierungsvorgänge aufgezeichnet und die Attestierungsvorgänge anschließend gelöscht. Es verbleiben genau so viele abgeschlossene Attestierungsvorgänge in der Datenbank, wie an den Attestierungsrichtlinien festgelegt ist. Ausführliche Informationen zum Aufzeichnen von Datenänderungen finden Sie im One Identity Manager Konfigurationshandbuch.

HINWEIS: Aus Gründen der Revisionssicherheit sollten Sie die aufgezeichneten Attestierungsvorgänge archivieren. Ausführliche Informationen zur Einrichtung eines Archivierungsverfahrens finden Sie im One Identity Manager Administrationshandbuch für die Datenarchivierung.

***Voraussetzungen***

- Der Konfigurationsparameter **Common | ProcessState | PropertyLog** ist aktiviert.
- Die Attestierungsrichtlinie ist aktiviert.

***Um Attestierungsvorgänge automatisiert zu löschen***

1. Aktivieren Sie an der Tabelle `AttestationCase` die Option **Aufzeichnen beim Löschen** für mindestens drei Spalten.
    a. Wählen Sie im Designer die Kategorie **Datenbankschema | Tabellen | AttestationCase**.
    b. Wählen Sie in der Aufgabenansicht **Tabellendefinition anzeigen**.

       Der Schemaeditor wird geöffnet.
    c. Wählen Sie im Schemaeditor eine Spalte.
    d. Wählen Sie in der Bearbeitungsansicht des Schemaeditors den Tabreiter **Sonstiges**.
    e. Aktivieren Sie die Option **Aufzeichnen beim Löschen**.
    f. Wiederholen Sie die Schritte c) bis e) für alle Spalten, die beim Löschen aufgezeichnet werden sollen, mindestens jedoch für drei Spalten.
    g. Klicken Sie **Übernahme in Datenbank** und speichern Sie die Änderungen.

       Sobald der DBQueue Prozessor die Berechnungsaufträge abgearbeitet hat, sind die Änderungen wirksam.
2. Aktivieren Sie an der Tabelle `AttestationHistory` die Option **Aufzeichnen beim Löschen** für mindestens drei Spalten.
    a. Wählen Sie im Designer die Kategorie **Datenbankschema | Tabellen | AttestationHistory**.
    b. Wiederholen Sie die Schritte 1b) bis 1g) für die Tabelle `AttestationHistory`.
3. Erfassen Sie an den Attestierungsrichtlinien die Anzahl veralteter Vorgänge.
    a. Wählen Sie im Manager die Kategorie **Attestierung | Attestierungsrichtlinien.**
    b. Wählen Sie in der Ergebnisliste die Attestierungsrichtlinie, deren

Attestierungsvorgänge gelöscht werden sollen.

c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

d. Erfassen Sie im Eingabefeld **Anzahl veralteter Vorgänge** einen Wert **größer 0**.

e. Speichern Sie die Änderungen.

TIPP: Wenn Sie verhindern wollen, dass für einzelne Attestierungsrichtlinien die Attestierungsvorgänge gelöscht werden, erfassen Sie als Anzahl veralteter Vorgänge für diese Attestierungsrichtlinien den Wert **0**.

Attestierungsvorgänge werden gelöscht, sobald

- für eine Attestierungsrichtlinie eine neue Attestierung gestartet wird.

  - ODER -

- eine Attestierungsrichtlinie deaktiviert wird.

Der One Identity Manager prüft, wie viele abgeschlossene Attestierungsvorgänge für jedes Attestierungsobjekt dieser Attestierungsrichtlinie in der Datenbank vorhanden sind. Wenn die Anzahl größer ist als die Anzahl veralteter Vorgänge der Attestierungsrichtlinie, werden

- die Eigenschaften dieser Attestierungsvorgänge und ihr Entscheidungsverlauf aufgezeichnet

  Es werden alle Spalten aufgezeichnet, die zum Aufzeichnen beim Löschen markiert sind.

- die Attestierungsvorgänge gelöscht

  Es verbleiben genau so viele abgeschlossene Attestierungsvorgänge in der Datenbank, wie in der Anzahl veralteter Vorgänge festgelegt ist.

HINWEIS: Für deaktivierte Attestierungsrichtlinien werden die abgeschlossenen Attestierungsvorgänge auch dann gelöscht, wenn der Konfigurationsparameter **Common | ProcessState | PropertyLog** deaktiviert ist. In diesem Fall werden die gelöschten Attestierungsvorgänge nicht aufgezeichnet.

### Verwandte Themen

- Allgemeine Stammdaten von Attestierungsrichtlinien auf Seite 28

# Benachrichtigungen im Attestierungsvorgang

Innerhalb eines Attestierungsvorgangs können verschiedene E-Mail Benachrichtigungen an Attestierer und andere Personen versendet 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 | Attestation | DefaultSenderAddress** und erfassen Sie die Absenderadresse, mit der die E-Mail Benachrichtigungen verschickt werden.
3. 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*.
4. 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*.
5. Konfigurieren Sie die Benachrichtigungsverfahren.

### Verwandte Themen

- Unternehmensspezifische Mailvorlagen für Benachrichtigungen auf Seite 38

# Aufforderung zur Attestierung

Liegt ein neuer Attestierungsvorgang vor, dann erhalten die Attestierer eine Benachrichtigung. Die Aufforderung zur Attestierung kann für jeden Entscheidungsschritt separat konfiguriert werden.

***Voraussetzung***

- Der Konfigurationsparameter **QER | Attestation | MailTemplateIdents | RequestApproverByCollection** ist deaktiviert.

***Um das Benachrichtigungsverfahren einzurichten***

- Erfassen Sie am Entscheidungsschritt auf dem Tabreiter **Mailvorlagen** die folgenden Daten.

  **Mailvorlage Aufforderung**: Attestierung - Aufforderung zur Entscheidung

TIPP: Um die Entscheidung per E-Mail zuzulassen, wählen Sie die Mailvorlage **Attestierung - Aufforderung zur Entscheidung (per E-Mail)**.

TIPP: Um eine allgemeine Benachrichtigung zu versenden, wenn offene Attestierungen vorliegen, können Sie die zeitgesteuerte Aufforderung zur Attestierung konfigurieren. Damit werden die einzelnen Aufforderungen zur Attestierung an den Entscheidungsschritten ersetzt.

### Verwandte Themen

- E-Mail-Benachrichtigung: Zeitgesteuerte Aufforderung zur Attestierung auf Seite 114
- Attestierung per E-Mail auf Seite 122
- Entscheidungsschritte bearbeiten auf Seite 55

# Erinnerung der Attestierer

Hat ein Attestierer nach Ablauf eines festgelegten Erinnerungsintervalls einen Attestierungsvorgang noch nicht bearbeitet, kann er eine Erinnerungsbenachrichtigung erhalten. Für die Zeitberechnung wird die gültige Arbeitszeit des Attestierers berücksichtigt.

***Voraussetzung***

- Der Konfigurationsparameter **QER | Attestation | MailTemplateIdents | RequestApproverByCollection** ist deaktiviert.

***Um das Benachrichtigungsverfahren einzurichten***

- Erfassen Sie am Entscheidungsschritt die folgenden Daten.

**Tabelle 35: Eigenschaften eines Entscheidungsschritts für Benachrichtungen**

| Eigenschaft | Bedeutung |
|---|---|
| Erinnerung nach (Arbeitsstunden) | Anzahl der Arbeitsstunden, nach deren Ablauf die Attestierer per E-Mail Benachrichtigung erinnert werden, dass noch offene Attestierungsvorgänge zur Attestierung vorliegen.<br>Das Erinnerungsintervall wird standardmäßig alle 30 Minuten geprüft. Um dieses Prüfintervall zu ändern, passen Sie den Zeitplan **Erinnerungsintervall und Timeout von Attestierungsvorgängen prüfen** an.<br>HINWEIS: Für die Ermittlung der gültigen Arbeitszeiten stellen Sie sicher, dass in den Stammdaten der Personen ein Bundesland und/oder ein Bundesstaat eingetragen ist. Wenn diese Informationen fehlen, wird ein Fallback zur Berechnung der Arbeitszeit genutzt. Ausführliche Informationen zur Ermittlung der Arbeitszeit von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.<br>Wurden mehrere Attestierer ermittelt, dann erhält jeder Attestierer die Benachrichtigung. Gleiches gilt, wenn ein zusätzlicher Attestierer beauftragt wurde.<br>Hat ein Attestierer die Entscheidung delegiert, wird der Zeitpunkt für die Erinnerung für den Empfänger der Delegierung neu berechnet. Der Empfänger der Delegierung und alle übrigen Attestierer erhalten die Benachrichtigung. Der ursprüngliche Attestierer wird nicht benachrichtigt.<br>Wenn ein Attestierer eine Anfrage gestellt hat, wird der Zeitpunkt für die Erinnerung für die angefragte Person neu berechnet. Solange die Anfrage nicht beantwortet ist, erhält nur diese Person die Benachrichtigung. |
| Mailvorlage Erinnerung | Wählen Sie die Mailvorlage **Attestierung - Erinnerung Entscheider**.<br>TIPP: Um die Entscheidung per E-Mail zuzulassen, wählen Sie die Mailvorlage **Attestierung - Erinnerung Entscheider (per E-Mail)**. |

TIPP:Um eine allgemeine Benachrichtigung zu versenden, wenn offene Attestierungen vorliegen, können Sie die zeitgesteuerte Aufforderung zur Attestierung konfigurieren. Damit werden die einzelnen Aufforderungen zur Attestierung an den Entscheidungsschritten ersetzt.

### Verwandte Themen

- E-Mail-Benachrichtigung: Zeitgesteuerte Aufforderung zur Attestierung auf Seite 114
- Attestierung per E-Mail auf Seite 122
- Entscheidungsschritte bearbeiten auf Seite 55

# Zeitgesteuerte Aufforderung zur Attestierung

Attestierer können regelmäßig darüber benachrichtigt werden, wenn für sie offene Attestierungsvorgänge vorliegen. Diese regelmäßigen Benachrichtigungen ersetzen die einzelnen Aufforderungen und Erinnerungen zur Attestierung, die am Entscheidungsschritt konfiguriert werden.

***Um regelmäßige Benachrichtigungen zu versenden, wenn offene Attestierungen vorliegen***

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | MailTemplateIdents | RequestApproverByCollection**.

   Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Attestierung - ausstehende Anträge für Entscheider** versendet.

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

2. Konfigurieren und aktivieren Sie im Designer den Zeitplan **Entscheider über ausstehende Attestierungen informieren**.

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

# Erinnerung der Attestierer von Attestierungsobjekten

Die Manager hierarchischer Rollen und die Verantwortlichen von Systemberechtigungen oder Systemrollen können im Web Portal alle offenen Attestierungsvorgänge für die Objekte sehen, für die sie verantwortlich sind. Bei Bedarf können sie Erinnerungsbenachrichtigungen an die Attestierer ausgewählter Attestierungsobjekte senden.

***Um eine Benachrichtigung für ein konkretes Attestierungsobjekt versenden zu können***

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | MailTemplateIdents | RemindApproverByObject**.

  Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Attestierung - Erinnerung Attestierer über alle offenen Attestierungen zu einem Objekt** versendet.

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

Um die Benachrichtigungen zu versenden, nutzen Sie das Web Portal. Ausführliche Informationen dazu finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

# Genehmigung oder Ablehnung von Attestierungsvorgängen

Bei Genehmigung oder Ablehnung eines Attestierungsvorgangs können weitere Personen eine Benachrichtigung erhalten. Diese Benachrichtigung kann bei Genehmigung oder Ablehnung eines einzelnen Entscheidungsschrittes oder bei Abschluss des gesamten Entscheidungsverfahrens erfolgen. Die Empfänger der Benachrichtigung legen Sie unternehmensspezifisch fest.

Attestierungsvorgänge können bei Überschreitung eines festgelegten Zeitraumes automatisch entschieden werden. Auch in diesem Fall wird eine Benachrichtigung versendet.

***Um das Benachrichtigungsverfahren einzurichten***

1. Erstellen Sie unternehmensspezifische Mailvorlagen für die Benachrichtigung bei Genehmigung und Ablehnung von Attestierungsvorgängen.
2. Erstellen Sie unternehmensspezifische Prozesse für Benachrichtigungen.
3. Wenn die Benachrichtigung gesendet werden soll, sobald ein einzelner Entscheidungsschritt entschieden wurde, erfassen Sie am Entscheidungsschritt auf dem Tabreiter **Mailvorlagen** die folgenden Daten.

**Tabelle 36: Eigenschaften eines Entscheidungsschritts für Benachrichtungen**

| Eigenschaft | Bedeutung |
|---|---|
| Mailvorlage Genehmigung | Mailvorlage, die für E-Mail Benachrichtigungen bei Genehmigung eines Entscheidungsschritts verwendet werden soll. |
| Mailvorlage Ablehnung | Mailvorlage, die für E-Mail Benachrichtigungen bei Ablehnung eines Entscheidungsschritts verwendet werden soll. |

- ODER -

Wenn die Benachrichtigung gesendet werden soll, sobald das gesamte Entscheidungsverfahren abgeschlossen ist, erfassen Sie an der Entscheidungsrichtlinie die folgenden Daten.

**Tabelle 37: Eigenschaften einer Entscheidungsrichtlinie für Benachrichtungen**

| Eigenschaft | Bedeutung |
|---|---|
| Mailvorlage Genehmigung | Mailvorlage, die für E-Mail Benachrichtigungen bei Genehmigung eines Attestierungsvorgangs verwendet werden soll. |
| Mailvorlage Ablehnung | Mailvorlage, die für E-Mail Benachrichtigungen bei Ablehnung eines Attestierungsvorgangs verwendet werden soll. |

### Detaillierte Informationen zum Thema

- Unternehmensspezifische Mailvorlagen für Benachrichtigungen auf Seite 38
- Unternehmensspezifische Prozesse für Benachrichtigungen auf Seite 45
- Entscheidungsschritte bearbeiten auf Seite 55
- Entscheidungsrichtlinien für Attestierungen auf Seite 46

# Benachrichtigung der Delegierenden

Ein Delegierender kann sich bei Bedarf benachrichtigen lassen, wenn der Empfänger der Delegierung einen Attestierungsvorgang entschieden hat. Eine Benachrichtigung wird versendet, sobald eine Person aufgrund einer Delegierung als Attestierer ermittelt wurde und den Attestierungsvorgang entschieden hat.

***Um eine Benachrichtigung zu versenden, wenn die Person, an die eine Entscheidung delegiert wurde, die Attestierung genehmigt oder abgelehnt hat***

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | Delegation | MailTemplateIdents | InformDelegatorAboutDecisionAttestation**.

  Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Delegierung - Entscheidung einer Attestierung** versendet.

HINWEIS: Um andere als die Standardmailvorlagen für diese Benachrichtigungen zu nutzen, ändern Sie die Werte der Konfigurationsparameter.

Delegierungen werden in folgenden Standard-Entscheidungsverfahren berücksichtigt.

**Tabelle 38: Für Delegierungen relevante Standard-Entscheidungsverfahren**

| Delegierung von | Entscheidungsverfahren |
|---|---|
| Verantwortungen für Abteilungen | DM, ED |
| Verantwortungen für Kostenstellen | PM |
| Verantwortungen für Standorte | LM |
| Verantwortungen für Geschäftsrollen | MO, OM, RM, RR |
| Verantwortungen für Personen | CM, EM |
| Mitgliedschaften in Geschäftsrollen | OR |
| Mitgliedschaften in Anwendungsrollen | AA, AD, AL, AN, AO, AP, AR, AS, AT, AY, EN, EO, OA, SO |

**Beispiel**

Jan Bloggs ist für die Geschäftsrolle R1 verantwortlich. Er delegiert seine Verantwortlichkeit für die Geschäftsrolle an Clara Harris. Clara Harris selbst ist für die Geschäftsrolle R2 verantwortlich.

Ein Mitglied der Geschäftsrolle R1 soll attestiert werden. Im Attestierungsverfahren wird über das Entscheidungsverfahren **OM - Manager einer bestimmten Rolle** Jan Bloggs als Attestierer ermittelt. Aufgrund der Delegierung wird Clara Harris der Attestierungsvorgang zur Entscheidung zugewiesen. Sobald Clara Harris über den Attestierungsvorgang entschieden hat, wird Jan Bloggs benachrichtigt.

Ein Mitglied der Geschäftsrolle R2 soll attestiert werden. Im Attestierungsverfahren wird über das Entscheidungsverfahren **OM - Manager einer bestimmten Rolle** Clara Harris als Attestierer ermittelt. Da Clara Harris die Entscheidung nicht aufgrund einer Delegierung trifft, wird keine Benachrichtigung versendet.

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

### Verwandte Themen

- Standard-Entscheidungsverfahren auf Seite 63
- Benachrichtigungen von zusätzlichen Attestierern auf Seite 120

# Abbruch von Attestierungsvorgängen

Bei Abbruch eines Attestierungsvorganges kann eine E-Mail Benachrichtigung an weitere Personen versendet werden. Die Empfänger der Benachrichtigung legen Sie

unternehmensspezifisch fest.

***Um das Benachrichtigungsverfahren einzurichten***

1. Erstellen Sie unternehmensspezifische Mailvorlagen für die Benachrichtigung bei Abbruch von Attestierungsvorgängen.
2. Erstellen Sie unternehmensspezifische Prozesse für Benachrichtigungen.
3. Erfassen Sie an der Entscheidungsrichtlinie die folgenden Daten.

   **Mailvorlage Abbruch**: Mailvorlage, die für E-Mail Benachrichtigungen bei Abbruch eines Attestierungsvorgangs verwendet werden soll.

### Detaillierte Informationen zum Thema

- Unternehmensspezifische Mailvorlagen für Benachrichtigungen auf Seite 38
- Unternehmensspezifische Prozesse für Benachrichtigungen auf Seite 45

# Eskalation von Attestierungsvorgängen

Bei Eskalation eines Attestierungsvorgangs kann eine E-Mail Benachrichtigung an den Eigentümer der Attestierungsrichtlinie versendet werden.

***Um das Benachrichtigungsverfahren einzurichten***

1. Erfassen Sie am Entscheidungsschritt auf dem Tabreiter **Mailvorlagen** die folgenden Daten.

   **Mailvorlage Eskalation**: Attestierung - Eskalation
2. Ordnen Sie den Attestierungsrichtlinien einen Eigentümer zu.

### Verwandte Themen

- Eskalieren eines Attestierungsvorgangs auf Seite 93
- Allgemeine Stammdaten von Attestierungsrichtlinien auf Seite 28
- Entscheidungsschritte bearbeiten auf Seite 55

# Delegierung von Attestierungen

Wenn an einem Entscheidungsschritt zusätzliche Attestierer mit der Entscheidung beauftragt werden, können die zusätzlichen Attestierer per E-Mail zur Entscheidung aufgefordert werden. Gleiches gilt, wenn die Attestierung delegiert werden kann.

***Um das Benachrichtigungsverfahren einzurichten***

- Erfassen Sie am Entscheidungsschritt auf dem Tabreiter **Mailvorlagen** die folgenden Daten.

  **Mailvorlage Delegierung**: Attestierung - Delegierte/zusätzliche Entscheidung

  TIPP: Um die Entscheidung per E-Mail zuzulassen, wählen Sie die Mailvorlage **Attestierung - Delegierte/zusätzliche Entscheidung (per E-Mail)**.

### Verwandte Themen

- Attestierung per E-Mail auf Seite 122
- Andere Attestierer beauftragen auf Seite 92
- Entscheidungsschritte bearbeiten auf Seite 55

# Zurückweisen von Entscheidungen

Wenn ein zusätzlicher Attestierer oder eine Person, an die eine Attestierung delegiert wird, die Entscheidung verweigert, soll der ursprüngliche Attestierer darüber benachrichtigt werden.

***Um das Benachrichtigungsverfahren einzurichten***

- Erfassen Sie am Entscheidungsschritt auf dem Tabreiter **Mailvorlagen** die folgenden Daten.

  **Mailvorlage Zurückweisung**: Attestierung - Ablehnung Entscheidung

  TIPP: Um die Entscheidung per E-Mail zuzulassen, wählen Sie die Mailvorlage **Attestierung - Ablehnung Entscheidung (per E-Mail)**.

### Verwandte Themen

- Attestierung per E-Mail auf Seite 122
- Andere Attestierer beauftragen auf Seite 92
- Entscheidungsschritte bearbeiten auf Seite 55

# Benachrichtigungen bei Anfragen

Personen können benachrichtigt werden, wenn eine Anfrage zu einer Attestierung gestellt wurde. Ebenso können die Attestierer benachrichtigt werden, sobald die Anfrage beantwortet wurde.

***Um eine Benachrichtigung zu versenden, wenn ein Attestierer eine Anfrage stellt***

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | MailTemplateIdents | QueryFromApprover**.

  Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Attestierung - Frage** versendet.

***Um eine Benachrichtigung an den Attestierer zu versenden, wenn die angefragte Person auf eine Anfrage antwortet***

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | MailTemplateIdents | AnswerToApprover**.

  Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Attestierung - Antwort** versendet.

HINWEIS: Um andere als die Standardmailvorlagen für diese Benachrichtigungen zu nutzen, ändern Sie die Werte der Konfigurationsparameter.

# Benachrichtigungen von zusätzlichen Attestierern

Der ursprüngliche Attestierer kann darüber benachrichtigt werden, dass ein zusätzlicher Attestierer oder eine Person, an die eine Attestierung delegiert wurde, die Attestierung genehmigt oder abgelehnt hat. Diese Benachrichtigung wird gesendet, sobald der Entscheidungsschritt entschieden wurde.

***Um eine Benachrichtigung zu versenden, wenn der zusätzliche Attestierer die Attestierung genehmigt oder abgelehnt hat***

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | MailTemplateIdents | InformAddingPerson**.

  Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Attestierung - Zusätzlicher Entscheidungsschritt entschieden** versendet.

***Um eine Benachrichtigung zu versenden, wenn die Person, an die eine Entscheidung delegiert wurde, die Attestierung genehmigt oder abgelehnt hat***

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | MailTemplateIdents | InformDelegatingPerson**.

  Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Attestierung - Delegierter Entscheidungsschritt entschieden** versendet.

HINWEIS: Um andere als die Standardmailvorlagen für diese Benachrichtigungen zu nutzen, ändern Sie die Werte der Konfigurationsparameter.

# Bestätigungslink für neue externe Benutzer

Wenn sich neue Benutzer am Web Portal registrieren oder wenn neue extern Personen zertifiziert werden sollen, erhalten diese Personen eine Mailbenachrichtigung, die einen Link zum Kennwortrücksetzungsportal enthält. Über diesen Link bestätigen die Personen ihre Kontakt-E-Mail-Adresse und setzen ein Kennwort und die Kennwortfragen.

***Um eine Benachrichtigung mit dem Bestätigungslink versenden zu können***

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | MailTemplateIdents | NewExternalUserVerification**.

  Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Attestierung - Bestätigungslink für neuen externen Benutzer** versendet.

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

### Detaillierte Informationen zum Thema

- Attestierung und Rezertifizierung von Benutzern auf Seite 136
- Selbstregistrierung neuer Benutzer im Web Portal auf Seite 139
- Anlegen neuer Personen durch einen Manager oder Personenadministrator auf Seite 142

# Standard-Mailvorlagen

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 **Attestierung | Basisdaten zur Konfiguration | Mailvorlagen | Vordefiniert**.

### Verwandte Themen

- Unternehmensspezifische Mailvorlagen für Benachrichtigungen auf Seite 38

# Attestierung per E-Mail

Um Attestierern, die zeitweilig keinen Zugang zu den One Identity Manager Werkzeugen haben, die Möglichkeit zu geben, Attestierungsvorgänge zu entscheiden, können Sie die Attestierung per E-Mail einrichten. Dabei erhalten die Attestierer eine E-Mail-Benachrichtigung, wenn für sie ein Attestierungsvorgang zur Entscheidung vorliegt. Über entsprechende Links in der E-Mail können die Attestierer die Entscheidung treffen, ohne sich mit dem Web Portal zu verbinden. Dabei wird eine E-Mail generiert, die die Entscheidung enthält und in der der Attestierer eine Begründung seiner Entscheidung erfassen soll. Diese E-Mail wird an ein zentrales Microsoft Exchange Postfach gesendet. Der One Identity Manager überprüft das Postfach regelmäßig, wertet die eingegangenen E-Mails aus und aktualisiert entsprechend den Status der Attestierungsvorgänge.

WICHTIG: Eine Attestierung per E-Mail ist nicht möglich, wenn für die Attestierungsrichtlinie die Multifaktor-Authentifizierung konfiguriert ist. Attestierungsmails für solche Attestierungen bewirken eine Fehlermeldung.

***Voraussetzungen***

1. Konfiguration der Microsoft Exchange Umgebung mit
   - Microsoft Exchange Client Access Server Version 2007, Service Pack 1 oder höher
   - Microsoft Exchange Web Service .NET API Version 1.2.1, 32 Bit
2. Das Benutzerkonto, mit dem sich der One Identity Manager Service an der Microsoft Exchange Umgebung anmeldet, benötigt Vollzugriff auf das Postfach, das im Konfigurationsparameter **QER | Attestation | MailApproval | Inbox** angegeben ist.
3. Der Konfigurationsparameter **QER | Attestation | MailTemplateIdents | RequestApproverByCollection** ist deaktiviert.

***Um die Attestierung per E-Mail einzurichten***

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | MailApproval | Inbox** und geben Sie das Postfach an, an das Entscheidungsmails gesendet werden sollen.
2. Richten Sie den Zugriff auf das Postfach ein.
   a. Standardmäßig nutzt der One Identity Manager das Benutzerkonto des One Identity Manager Service, um sich am Microsoft Exchange Server anzumelden und auf das Postfach zuzugreifen.

      - ODER -

   b. Geben Sie ein separates Benutzerkonto für die Anmeldung am Microsoft Exchange Server zum Zugriff auf das Postfach an. Aktivieren Sie dafür die folgenden Konfigurationsparameter.

**Tabelle 39: Konfigurationsparameter für die Anmeldung am Microsoft Exchange Server**

| Konfigurationsparameter | Bedeutung |
|---|---|
| QER \| Attestation \| MailApproval \| Account | Name des Benutzerkontos. |
| QER \| Attestation \| MailApproval \| Domain | Domäne des Benutzerkontos. |
| QER \| Attestation \| MailApproval \| Password | Kennwort des Benutzerkontos. |

3. Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | MailTemplateIdents | ITShopApproval**.

   An diesem Konfigurationsparameter ist die Mailvorlage hinterlegt, die genutzt wird, um die Attestierungsmail zu erstellen. Sie können die Standardmailvorlage nutzen oder eine unternehmensspezifische Mailvorlage hinterlegen.

   TIPP: Um eine unternehmensspezifische Mailvorlage für Attestierungsmails zu nutzen, ändern Sie den Wert des Konfigurationsparameters. Passen Sie in diesem Fall auch das Skript `VI_MailApproval_ProcessMail` an.

4. Ordnen Sie an den Entscheidungsschritten folgende Mailvorlagen zu.

**Tabelle 40: Mailvorlagen für die Entscheidung per E-Mail**

| Eigenschaft | Mailvorlage |
|---|---|
| Mailvorlage Aufforderung | Attestierung - Aufforderung zur Entscheidung (per E-Mail) |
| Mailvorlage Erinnerung | Attestierung - Erinnerung Entscheider (per E-Mail) |
| Mailvorlage Delegierung | Attestierung - Delegierte/zusätzliche Entscheidung (per E-Mail) |
| Mailvorlage Zurückweisung | Attestierung - Ablehnung Entscheidung (per E-Mail) |

5. Konfigurieren und aktivieren Sie im Designer den Zeitplan **Verarbeiten der Entscheidungen von Attestierungen per E-Mail**.

   Entsprechend diesem Zeitplan überprüft der One Identity Manager regelmäßig das Postfach nach neuen Attestierungsmails. Standardmäßig wird das Postfach alle 15 Minuten überprüft. Sie können das Ausführungsintervall des Zeitplans entsprechend ihren Erfordernissen anpassen.

***Um das Postfach aufzuräumen***

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | MailApproval | DeleteMode** und wählen Sie einen der folgenden Werte.

**Tabelle 41: Aufräumen eines Postfachs**

| Wert | Verfahren |
|---|---|
| HardDelete | Die verarbeitete E-Mail wird sofort gelöscht. |
| MoveToDeletedItems | Die verarbeitete E-Mail wird in den Ordner **Gelöschte Objekte** des Postfachs verschoben. |
| SoftDelete | Die verarbeitete E-Mail wird in den Active Directory Papierkorb verschoben und kann bei Bedarf wiederhergestellt werden. |

HINWEIS: Bei Einsatz der Aufräumverfahren MoveToDeletedItems oder SoftDelete sollten Sie den Ordner **Gelöschte Objekte** und den Active Directory Papierkorb in regelmäßigen Abständen leeren.

### Verwandte Themen

- Verarbeitung von Attestierungsmails auf Seite 124
- Unternehmensspezifische Mailvorlagen für Benachrichtigungen auf Seite 38
- Aufforderung zur Attestierung auf Seite 111
- Erinnerung der Attestierer auf Seite 112
- Delegierung von Attestierungen auf Seite 118
- Zurückweisen von Entscheidungen auf Seite 119
- Einrichten der Multifaktor-Authentifizierung für Attestierungen auf Seite 89

# Verarbeitung von Attestierungsmails

Der Zeitplan **Verarbeiten der Entscheidungen von Attestierungen per E-Mail** startet den Prozess VI_Attestation_Process Approval Inbox. Dieser Prozess führt das Skript VI_MailApproval_ProcessInBox aus, welches das Postfach nach neuen Attestierungsmails durchsucht und die Attestierungsvorgänge in der One Identity Manager-Datenbank aktualisiert. Dabei wird der Inhalt der Attestierungsmail verarbeitet.

HINWEIS: Die Gültigkeit der Serverzertifikate wird durch das Skript VID_ValidateCertificate überprüft. Sie können dieses Skript an Ihre unternehmensspezifischen Sicherheitsanforderungen anpassen. Beachten Sie dabei, dass dieses Skript auch für Attestierungen per E-Mail verwendet wird!

Wird eine nicht öffentlich signierte Root CA/Zertifizierungsstelle verwendet, so muss das Benutzerkonto unter dem der One Identity Manager Service läuft, diesem Rootzertifikat vertrauen.

TIPP: Das Skript `VI_MailApproval_ProcessInBox` ermittelt die Exchange Web Service URL standardmäßig per AutoDiscover über das übergebene Postfach. Dies setzt voraus, dass der Autodiscover-Dienst läuft.

Falls das nicht möglich ist, geben Sie die URL im Konfigurationsparameter QER\Attestation\MailApproval\ExchangeURI an.

Attestierungsmails werden durch das Skript `VI_MailApproval_ProcessMail` verarbeitet. Das Skript ermittelt die getroffene Entscheidung, aktiviert bei positiver Entscheidung die Option **Genehmigt** und hinterlegt die Begründung für die Entscheidung an den Attestierungsvorgängen. Über die Absenderadresse wird der Attestierer ermittelt. Danach wird die Attestierungsmail abhängig vom gewählten Aufräumverfahren aus dem Postfach entfernt.

HINWEIS: Wenn Sie eine unternehmensspezifische Mailvorlage für die Attestierungsmail nutzen, prüfen Sie das Skript und passen Sie es gegebenenfalls an. Beachten Sie dabei, dass dieses Skript auch für Entscheidungen von IT Shop-Bestellungen per E-Mail verwendet wird!

# 4

# Standardattestierungen und der Entzug von Berechtigungen

Der One Identity Manager stellt für verschiedene Datensituationen Standard-Attestierungsverfahren und Standard-Attestierungsrichtlinien bereit.

Datensituationen für Standardattestierungen:

- Systemberechtigungen, die eine Person besitzt
- Systemberechtigungen, die an Systemberechtigungen zugewiesen sind
- Systemberechtigungen, die an hierarchische Rollen zugewiesen sind
- Systemrollen, die einer Person zugewiesen sind
- Unternehmensressourcen, die an Systemrollen zugewiesen sind
- Systemrollen, die an hierarchische Rollen zugewiesen sind
- Mitgliedschaften in Geschäftsrollen und Anwendungsrollen
- Personenstammdaten eines neuen One Identity Manager Benutzers
- Personenstammdaten vorhandener One Identity Manager Benutzer

Für die Attestierung von Personenstammdaten werden die erforderlichen Attestierungsrichtlinien standardmäßig bereitgestellt. Sie können diese Attestierungsrichtlinien ohne weitere Anpassungen nutzen. Voraussetzungen und Ablauf der Attestierung von Personenstammdaten ist im Abschnitt Attestierung und Rezertifizierung von Benutzern beschrieben.

Mit den Standard-Attestierungsverfahren für die übrigen Datensituationen können Sie auf einfachem Wege im Web Portal Attestierungsrichtlinien erstellen. Sie können auch die mitgelieferten Standard-Attestierungsrichtlinien ohne weitere Anpassungen nutzen. Darüber hinaus können Sie konfigurieren, wie mit abgelehnten Attestierungen weiter verfahren werden soll, die auf diesen Standard-Attestierungsverfahren basieren. Wenn es Ihre spezielle Datensituation zulässt, können abgelehnte Berechtigungen sofort im Anschluss an die Attestierung durch den One Identity Manager entzogen werden.

***Um abgelehnte Berechtigungen automatisch zu entziehen***

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | AutoRemovalScope** und die untergeordneten Konfigurationsparameter.
2. Wenn die Berechtigungen über IT Shop Bestellungen erworben wurden, legen Sie fest, ob diese Bestellungen abbestellt oder abgebrochen werden sollen. Aktivieren Sie dafür den Konfigurationsparameter **QER | Attestation | AutoRemovalScope | PWOMethodName** und wählen Sie einen Wert.
   - **Abort**: Bestellungen werden abgebrochen. Sie durchlaufen damit keinen Abbestellworkflow. Die bestellten Berechtigungen werden ohne zusätzliche Prüfung entzogen.
   - **Unsubscribe**: Bestellungen werden abbestellt. Sie durchlaufen den an den Entscheidungsrichtlinien hinterlegten Abbestellworkflow. Der Entzug der Berechtigung kann damit zusätzlich geprüft werden.

     Wenn die Abbestellung abgelehnt wird, wird die Berechtigung nicht entzogen, obwohl die Attestierung abgelehnt ist.

   Wenn der Konfigurationsparameter deaktiviert ist, werden die Bestellungen abgebrochen.

WICHTIG: Wenn einer Person Rollenmitgliedschaften oder Systemrollen entzogen werden, verliert sie dadurch die abgelehnte Berechtigung. Sie verliert aber auch alle anderen Unternehmensressourcen, die ihr über die Rolle vererbt wurden. Das können weitere Systemberechtigungen oder Kontendefinitionen sein. Gegebenenfalls werden ihr dadurch zulässige Systemberechtigungen entzogen oder Benutzerkonten gelöscht!

Prüfen sie, ob Ihre Datensituation den automatischen Entzug von Berechtigungen zulässt, bevor Sie die Konfigurationsparameter unter **QER | Attestation | AutoRemovalScope** aktivieren.

Der automatische Entzug von Berechtigungen wird durch einen zusätzlichen Entscheidungsschritt mit dem Entscheidungsverfahren EX in den Standard-Entscheidungsworkflows angestoßen.

Ablauf der Attestierung mit anschließendem Entzug abgelehnter Berechtigungen:

1. Eine Attestierung mit einem Standard-Attestierungsverfahren wird durchgeführt.
2. Der Attestierer lehnt die Attestierung ab. Der Entscheidungsschritt wird negativ entschieden und die Entscheidung an die nächste Entscheidungsebene mit dem Entscheidungsverfahren EX übergeben.
3. Der Entscheidungsschritt löst das Ereignis `AUTOREMOVE` aus. Dadurch wird der Prozess `VI_Attestation_AttestationCase_AutoRemoveMemberships` ausgeführt.
4. Der Prozess führt das Skript `VI_AttestationCase_RemoveMembership` aus. Dieses entfernt die betroffene Berechtigung abhängig von den aktivierten Konfigurationsparametern.
5. Das Skript setzt den Status des Entscheidungsschritts auf **Abgelehnt**. Dadurch wird der gesamte Attestierungsvorgang endgültig abgelehnt.
6. Aufträge zur Neuberechnung der Vererbung werden in die DBQueue eingestellt.

### Detaillierte Informationen zum Thema

- Attestierung von Systemberechtigungen auf Seite 128
- Attestierung von Systemrollen auf Seite 131
- Attestierung von Anwendungsrollen auf Seite 133
- Attestierung von Geschäftsrollen auf Seite 134

# Attestierung von Systemberechtigungen

Installierte Module: Zielsystem Basismodul

Wenn Sie die Standard-Attestierungsrichtline **Attestierung von Mitgliedschaften in Systemberechtigungen** nutzen oder Attestierungsrichtlinien mit dem Standard-Attestierungsverfahren **Attestierung von Mitgliedschaften in Systemberechtigungen** erstellt haben, können Sie den automatischen Entzug der Systemberechtigungen über den Konfigurationsparameter **QER | Attestation | AutoRemovalScope | GroupMembership** konfigurieren. Der One Identity Manager prüft im Anschluss an eine abgelehnte Attestierung, über welche Zuweisungsart das Benutzerkonto Mitglied in der Systemberechtigung wurde.

**Tabelle 42: Wirkung der Konfigurationsparameter bei abgelehnter Attestierung**

| Konfigurationsparameter | Wirkung bei Aktivierung |
|---|---|
| QER \| Attestation \| AutoRemovalScope \| GroupMembership \| RemoveDirect | Die direkte Mitgliedschaft des Benutzerkontos in der Systemberechtigung wird entfernt. |
| QER \| Attestation \| AutoRemovalScope \| GroupMembership \| RemovePrimaryRole | Wurde die Mitgliedschaft in der Systemberechtigung über eine primäre Rolle vererbt, wird der Person diese Rolle entzogen.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Rolle erhalten hat. |
| QER \| Attestation \| AutoRemovalScope \| GroupMembership \| RemoveRequestedRole | Wurde die Mitgliedschaft in der Systemberechtigung über eine bestellte Rolle vererbt, wird die Bestellung der Rolle abgebrochen oder abbestellt.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Rolle erhalten hat.<br>Das gewünschte Verhalten stellen Sie am Konfigurationsparameter **QER \| Attestation \| AutoRe-** |

| Konfigurationsparameter | Wirkung bei Aktivierung |
|---|---|
| | **movalScope \| PWOMethodName** ein. Weitere Informationen finden Sie unter Standardattestierungen und der Entzug von Berechtigungen auf Seite 126. |
| QER \| Attestation \| AutoRemovalScope \| GroupMembership \| RemoveDelegatedRole | Wurde die Mitgliedschaft in der Systemberechtigung über eine delegierte Rolle vererbt, wird die Delegierung dieser Rolle abgebrochen oder abbestellt.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Rolle erhalten hat.<br>Das gewünschte Verhalten stellen Sie am Konfigurationsparameter **QER \| Attestation \| AutoRemovalScope \| PWOMethodName** ein. Weitere Informationen finden Sie unter Standardattestierungen und der Entzug von Berechtigungen auf Seite 126. |
| QER \| Attestation \| AutoRemovalScope \| GroupMembership \| RemoveRequested | Wurde die Mitgliedschaft in der Systemberechtigung über den IT Shop bestellt, wird die Bestellung abgebrochen oder abbestellt.<br>Das gewünschte Verhalten stellen Sie am Konfigurationsparameter **QER \| Attestation \| AutoRemovalScope \| PWOMethodName** ein. Weitere Informationen finden Sie unter Standardattestierungen und der Entzug von Berechtigungen auf Seite 126. |
| QER \| Attestation \| AutoRemovalScope \| GroupMembership \| RemoveSystemRole | Systemrollen, welche die Systemberechtigung enthalten, werden der Person entzogen.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Systemrolle erhalten hat.<br>Dieser Konfigurationsparameter ist nur verfügbar, wenn das Systemrollenmodul installiert ist. |
| QER \| Attestation \| AutoRemovalScope \| GroupMembership \| RemoveDirectRole | Die Zuweisung der Systemberechtigung an hierarchische Rollen wird entfernt.<br>Damit wird die Zuweisung der Systemberechtigung zu allen Benutzerkonten entfernt, deren verbundene Personen die Zuweisungen von diesen Rollen erben.<br>WICHTIG: Dadurch können auch Benutzerkonten die Systemberechtigung verlieren, deren Attestierung genehmigt wurde.<br>Prüfen Sie die Nebenwirkungen dieses Konfigurationsparameters in Ihrer Datensituation, bevor Sie ihn aktivieren. |

Wenn Sie die Standard-Attestierungsrichtline **Attestierung von Zuweisungen zu Systemberechtigungen** nutzen oder Attestierungsrichtlinien mit dem Standard-

Attestierungsverfahren **Attestierung der Zuweisung von Systemberechtigungen an Systemberechtigungen** erstellt haben, können Sie den automatischen Entzug der Systemberechtigungen über den Konfigurationsparameter **QER | Attestation | AutoRemovalScope | UNSGroupInUNSGroup** konfigurieren.

**Tabelle 43: Wirkung des Konfigurationsparameters bei abgelehnter Attestierung**

| Konfigurationsparameter | Wirkung bei Aktivierung |
|---|---|
| QER \| Attestation \| AutoRemovalScope \| UNSGroupInUNSGroup \| RemoveDirect | Die Zuweisung der Systemberechtigung an eine Systemberechtigung wird entfernt. |

Der automatische Entzug der Zuweisung von Systemberechtigungen an hierarchische Rollen kann konfiguriert werden, wenn Sie folgende Standard-Attestierungsrichtlinien oder Standard-Attestierungsverfahren nutzen:

- Attestierung der Zuweisung von Systemberechtigungen an Abteilungen
- Attestierung der Zuweisung von Systemberechtigungen an Kostenstellen
- Attestierung der Zuweisung von Systemberechtigungen an Standorte
- Attestierung der Zuweisung von Systemberechtigungen an Geschäftsrollen

Aktivieren Sie dafür die folgenden Konfigurationsparameter.

**Tabelle 44: Wirkung der Konfigurationsparameter bei abgelehnter Attestierung**

| Konfigurationsparameter | Wirkung bei Aktivierung |
|---|---|
| QER \| Attestation \| AutoRemovalScope \| DepartmentHasUNSGroup \| RemoveDirect | Die Zuweisung der Systemberechtigung an eine Abteilung wird entfernt.<br>Damit wird allen Personen, die Zuweisungen von dieser Abteilung erben, die Systemberechtigung entzogen. |
| QER \| Attestation \| AutoRemovalScope \| ProfitCenterHasUNSGroup \| RemoveDirect | Die Zuweisung der Systemberechtigung an eine Kostenstelle wird entfernt.<br>Damit wird allen Personen, die Zuweisungen von dieser Kostenstelle erben, die Systemberechtigung entzogen. |
| QER \| Attestation \| AutoRemovalScope \| LocalityHasUNSGroup \| RemoveDirect | Die Zuweisung der Systemberechtigung an einen Standort wird entfernt.<br>Damit wird allen Personen, die Zuweisungen von diesem Standort erben, die Systemberechtigung entzogen. |
| QER \| Attestation \| AutoRemovalScope \| OrgHasUNSGroup \| RemoveDirect | Die Zuweisung der Systemberechtigung an eine Geschäftsrolle wird entfernt.<br>Damit wird allen Personen, die Zuweisungen von dieser Geschäftsrolle erben, die Systemberechtigung entzogen. |

# Attestierung von Systemrollen

Installierte Module: Systemrollenmodul

Wenn Sie die Standard-Attestierungsrichtline **Attestierung von Mitgliedschaften in Systemrollen** nutzen oder Attestierungsrichtlinien mit dem Standard-Attestierungsverfahren **Attestierung von Mitgliedschaften in Systemrollen** erstellt haben, können Sie den automatischen Entzug der Systemrollen über den Konfigurationsparameter **QER | Attestation | AutoRemovalScope | ESetAssignment** konfigurieren. Der One Identity Manager prüft im Anschluss an eine abgelehnte Attestierung, über welche Zuweisungsart die Person die Systemrolle erhalten hat.

**Tabelle 45: Wirkung der Konfigurationsparameter bei abgelehnter Attestierung**

| Konfigurationsparameter | Wirkung bei Aktivierung |
|---|---|
| QER \| Attestation \| AutoRemovalScope \| ESetAssignment \| RemoveDirect | Die direkte Mitgliedschaft in der Systemrolle wird entfernt.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Systemrolle erhalten hat. |
| QER \| Attestation \| AutoRemovalScope \| ESetAssignment \| RemovePrimaryRole | Wurde die Systemrolle über eine primäre Rolle vererbt, wird der Person diese Rolle entzogen.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Rolle erhalten hat. |
| QER \| Attestation \| AutoRemovalScope \| ESetAssignment \| RemoveRequestedRole | Wurde die Systemrolle über eine bestellte Rolle vererbt, wird die Bestellung der Rolle abgebrochen oder abbestellt.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Rolle erhalten hat.<br>Das gewünschte Verhalten stellen Sie am Konfigurationsparameter **QER \| Attestation \| AutoRemovalScope \| PWOMethodName** ein. Weitere Informationen finden Sie unter Standardattestierungen und der Entzug von Berechtigungen auf Seite 126. |
| QER \| Attestation \| AutoRemovalScope \| ESetAssignment \| RemoveDelegatedRole | Wurde die Systemrolle über eine delegierte Rolle vererbt, wird die Delegierung dieser Rolle abgebrochen oder abbestellt.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Rolle erhalten hat.<br>Das gewünschte Verhalten stellen Sie am Konfigurationsparameter **QER \| Attestation \| AutoRemovalScope \| PWOMethodName** ein. Weitere Informationen finden Sie unter Standardattestierungen und der Entzug von Berechtigungen auf Seite 126. |

| Konfigurationsparameter | Wirkung bei Aktivierung |
|---|---|
| QER \| Attestation \| AutoRemovalScope \| ESetAssignment \| RemoveRequested | Wurde die Systemrolle über den IT Shop bestellt, wird die Bestellung abgebrochen oder abbestellt.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Systemrolle erhalten hat.<br>Das gewünschte Verhalten stellen Sie am Konfigurationsparameter **QER \| Attestation \| AutoRemovalScope \| PWOMethodName** ein. Weitere Informationen finden Sie unter Standardattestierungen und der Entzug von Berechtigungen auf Seite 126. |
| QER \| Attestation \| AutoRemovalScope \| ESetAssignment \| RemoveDirectRole | Die Zuweisung der Systemrolle an hierarchische Rollen wird entfernt.<br>Damit wird die Zuweisung der Systemrolle zu allen Personen entfernt, die Zuweisungen von diesen Rollen erben.<br>WICHTIG: Dadurch können auch Personen die Systemrolle verlieren, deren Attestierung genehmigt wurde.<br>Prüfen Sie die Nebenwirkungen dieses Konfigurationsparameters in Ihrer Datensituation, bevor Sie ihn aktivieren. |

Wenn Sie die Standard-Attestierungsrichtline **Attestierung von Zuweisungen an Systemrollen** nutzen oder Attestierungsrichtlinien mit dem Standard-Attestierungsverfahren **Attestierung von Zuweisungen an Systemrollen** erstellt haben, können Sie den automatischen Entzug der Zuweisungen über den Konfigurationsparameter **QER \| Attestation \| AutoRemovalScope \| ESetHasEntitlement** konfigurieren.

**Tabelle 46: Wirkung des Konfigurationsparameters bei abgelehnter Attestierung**

| Konfigurationsparameter | Wirkung bei Aktivierung |
|---|---|
| QER \| Attestation \| AutoRemovalScope \| ESetHasEntitlement \| RemoveDirect | Die Zuweisung der Unternehmensressource an eine Systemrolle wird entfernt. |

Der automatische Entzug der Zuweisung von Systemrollen an hierarchische Rollen kann konfiguriert werden, wenn Sie folgende Standard-Attestierungsrichtlinien oder Standard-Attestierungsverfahren nutzen:

- Attestierung der Zuweisung von Systemrollen an Abteilungen
- Attestierung der Zuweisung von Systemrollen an Kostenstellen
- Attestierung der Zuweisung von Systemrollen an Standorte
- Attestierung der Zuweisung von Systemrollen an Geschäftsrollen

Aktivieren Sie dafür die folgenden Konfigurationsparameter.

**Tabelle 47: Wirkung der Konfigurationsparameter bei abgelehnter Attestierung**

| Konfigurationsparameter | Wirkung bei Aktivierung |
|---|---|
| QER \| Attestation \| AutoRemovalScope \| DepartmentHasESet \| RemoveDirect | Die Zuweisung der Systemrolle an eine Abteilung wird entfernt.<br>Damit wird allen Personen, die Zuweisungen von dieser Abteilung erben, die Systemrolle entzogen. |
| QER \| Attestation \| AutoRemovalScope \| ProfitCenterHasESet \| RemoveDirect | Die Zuweisung der Systemrolle an eine Kostenstelle wird entfernt.<br>Damit wird allen Personen, die Zuweisungen von dieser Kostenstelle erben, die Systemrolle entzogen. |
| QER \| Attestation \| AutoRemovalScope \| LocalityHasESet \| RemoveDirect | Die Zuweisung der Systemrolle an einen Standort wird entfernt.<br>Damit wird allen Personen, die Zuweisungen von diesem Standort erben, die Systemrolle entzogen. |
| QER \| Attestation \| AutoRemovalScope \| OrgHasESet \| RemoveDirect | Die Zuweisung der Systemrolle an eine Geschäftsrolle wird entfernt.<br>Damit wird allen Personen, die Zuweisungen von dieser Geschäftsrolle erben, die Systemrolle entzogen. |

# Attestierung von Anwendungsrollen

Wenn Sie die Standard-Attestierungsrichtline **Attestierung von Mitgliedschaften in Anwendungsrollen** nutzen oder Attestierungsrichtlinien mit dem Standard-Attestierungsverfahren **Attestierung von Mitgliedschaften in Anwendungsrollen** erstellt haben, können Sie den automatischen Entzug der Anwendungsrollen über den Konfigurationsparameter **QER \| Attestation \| AutoRemovalScope \| AERoleMembership** konfigurieren. Der One Identity Manager prüft im Anschluss an eine abgelehnte Attestierung, über welche Zuweisungsart die Person Mitglied in der Anwendungsrolle wurde.

**Tabelle 48: Wirkung der Konfigurationsparameter bei abgelehnter Attestierung**

| Konfigurationsparameter | Wirkung bei Aktivierung |
|---|---|
| QER \| Attestation \| AutoRemovalScope \| AERoleMembership \| RemoveDirectRole | Die sekundäre Mitgliedschaft der Person in der Anwendungsrolle wird entfernt.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Anwendungsrolle erhalten hat. Mitgliedschaften in dynamischen Rollen werden |

| Konfigurationsparameter | Wirkung bei Aktivierung |
|---|---|
| | dadurch nicht entfernt. |
| QER \| Attestation \| AutoRemovalScope \| AERoleMembership \| RemoveRequestedRole | Hat die Person die Anwendungsrolle über den IT Shop bestellt, wird die Bestellung abgebrochen oder abbestellt.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Anwendungsrolle erhalten hat.<br>Das gewünschte Verhalten stellen Sie am Konfigurationsparameter **QER \| Attestation \| AutoRemovalScope \| PWOMethodName** ein. Weitere Informationen finden Sie unter Standardattestierungen und der Entzug von Berechtigungen auf Seite 126. |
| QER \| Attestation \| AutoRemovalScope \| AERoleMembership \| RemoveDelegatedRole | Wurde die Anwendungsrolle an die Person delegiert, wird die Delegierung abgebrochen oder abbestellt.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Anwendungsrolle erhalten hat.<br>Das gewünschte Verhalten stellen Sie am Konfigurationsparameter **QER \| Attestation \| AutoRemovalScope \| PWOMethodName** ein. Weitere Informationen finden Sie unter Standardattestierungen und der Entzug von Berechtigungen auf Seite 126. |

# Attestierung von Geschäftsrollen

Installierte Module: Geschäftsrollenmodul

Wenn Sie die Standard-Attestierungsrichtline **Attestierung von Mitgliedschaften in Geschäftsrollen** nutzen oder Attestierungsrichtlinien mit dem Standard-Attestierungsverfahren **Attestierung von Mitgliedschaften in Geschäftsrollen** erstellt haben, können Sie den automatischen Entzug der Geschäftsrollen über den Konfigurationsparameter **QER \| Attestation \| AutoRemovalScope \| RoleMembership** konfigurieren. Der One Identity Manager prüft im Anschluss an eine abgelehnte Attestierung, über welche Zuweisungsart die Person Mitglied in der Geschäftsrolle wurde.

**Tabelle 49: Wirkung der Konfigurationsparameter bei abgelehnter Attestierung**

| Konfigurationsparameter | Wirkung bei Aktivierung |
|---|---|
| QER \| Attestation \| AutoRemovalScope \| RoleMembership \| | Die sekundäre Mitgliedschaft der Person in der Geschäftsrolle wird entfernt. |

| Konfigurationsparameter | Wirkung bei Aktivierung |
|---|---|
| RemoveDirectRole | Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Geschäftsrolle erhalten hat. Mitgliedschaften in dynamischen Rollen werden dadurch nicht entfernt! |
| QER \| Attestation \| AutoRemovalScope \| RoleMembership \| RemoveRequestedRole | Hat die Person die Geschäftsrolle über den IT Shop bestellt, wird die Bestellung abgebrochen oder abbestellt.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Geschäftsrolle erhalten hat.<br>Das gewünschte Verhalten stellen Sie am Konfigurationsparameter **QER \| Attestation \| AutoRemovalScope \| PWOMethodName** ein. Weitere Informationen finden Sie unter Standardattestierungen und der Entzug von Berechtigungen auf Seite 126. |
| QER \| Attestation \| AutoRemovalScope \| RoleMembership \| RemoveDelegatedRole | Wurde die Geschäftsrolle an die Person delegiert, wird die Delegierung abgebrochen oder abbestellt.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Geschäftsrolle erhalten hat.<br>Das gewünschte Verhalten stellen Sie am Konfigurationsparameter **QER \| Attestation \| AutoRemovalScope \| PWOMethodName** ein. Weitere Informationen finden Sie unter Standardattestierungen und der Entzug von Berechtigungen auf Seite 126. |

# 5

# Attestierung und Rezertifizierung von Benutzern

Über die Attestierungsfunktion des One Identity Manager können die Stammdaten von Personen sowie deren Zielsystemberechtigungen und Zuweisungen regelmäßig überprüft und autorisiert werden. Darüber hinaus stellt der One Identity Manager Standardverfahren bereit, über welche die Stammdaten von One Identity Manager Benutzern, die neu in die One Identity Manager-Datenbank aufgenommen wurden, zeitnah durch deren Manager attestiert und zertifiziert werden. Diese Funktionalität kann beispielsweise genutzt werden, wenn externen Mitarbeitern zeitweilig Zugang zum One Identity Manager gewährt werden soll. Für interne und externe Personen gelten jeweils unterschiedliche Abläufe.

Über zeitgesteuerte Aufträge kann eine regelmäßige Rezertifizierung durchgeführt werden.

Im Rahmen der Attestierung kann ein Manager die Personenstammdaten des zu zertifizierenden Benutzers prüfen und bei Bedarf aktualisieren. Für Attestierungen nutzen Sie das Web Portal.

### Detaillierte Informationen zum Thema

- Attestierung und Rezertifizierung von Benutzern konfigurieren auf Seite 138
- Attestierung neuer Benutzer auf Seite 139
- Rezertifizierung vorhandener Benutzer auf Seite 148

# One Identity Manager Benutzer für die Attestierung und Rezertifizierung von Benutzern

In die Attestierung und Rezertifizierung von Personen sind folgende Benutzer eingebunden.

**Tabelle 50: Benutzer**

| Benutzer | Aufgaben |
|---|---|
| Personenadministratoren | Personenadministratoren müssen der Anwendungsrolle **Identity Management \| Personen \| Administratoren** zugewiesen sein.<br>Benutzer mit dieser Anwendungsrolle:<br>• Bearbeiten die Stammdaten aller Personen.<br>• Ordnen den Manager zu.<br>• Weisen Unternehmensressourcen an die Personen zu.<br>• Überprüfen und autorisieren die Stammdaten von Personen.<br>• Erstellen und bearbeiten Risikoindex-Berechnungsvorschriften.<br>• Bearbeiten Kennwortrichtlinien für Kennwörter von Personen.<br>• Können Sicherheitsschlüssel (Webauthn) von Personen löschen. |
| Manager | • Prüfen die Personenstammdaten der zu zertifizierenden Benutzer.<br>• Aktualisieren bei Bedarf die Personenstammdaten.<br>• Ordnen gegebenenfalls einen anderen Manager zu.<br>• Attestieren die Stammdaten. |
| Attestierer für externe Benutzer | Die Attestierer für externe Benutzer müssen der Anwendungsrolle **Identity & Access Governance \| Attestierung \| Attestierer für externe Benutzer** zugewiesen sein.<br>Benutzer mit dieser Anwendungsrolle:<br>• Attestieren neue externe Personen. |
| Administratoren für Attestierungsvorgänge | Administratoren für die Attestierungsvorgänge müssen der Anwendungsrolle **Identity & Access Governance \| Attestierung \| Administratoren** zugewiesen sein.<br>Benutzer mit dieser Anwendungsrolle:<br>• Passen gegebenenfalls die Attestierungsrichtlinien an.<br>• Erstellen bei Bedarf weitere Zeitpläne. |
| Web Portal Benutzer | • Registrieren sich am Web Portal und erfassen ihre Stammdaten. |

# Attestierung und Rezertifizierung von Benutzern konfigurieren

***Um die Attestierungs- und Rezertifizierungsfunktion für neue interne Benutzer nutzen zu können***

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | Attestation | UserApproval**.
2. Weisen Sie der Anwendungsrolle **Identity Management | Personen | Administratoren** mindestens eine Person zu.

   Alle Personen mit dieser Anwendungsrolle können im Verlauf der Attestierung einen Manager an die zu attestierenden Personen zuordnen.

***Um die Attestierungs- und Rezertifizierungsfunktion für neue externe Benutzer nutzen zu können***

1. Aktivieren Sie im Designer die folgenden Konfigurationsparameter:
   - **QER | Attestation | ApproveNewExternalUsers**: Wählen Sie den Wert **1**.
   - **QER | WebPortal | PasswordResetURL**: Geben Sie als Wert die URL zum Kennwortrücksetzungsportal an.
   - **QER | Attestation | MailTemplateIdents | NewExternalUserVerification**: Mailvorlage für den Versand des Bestätigungslinks.
   - **QER | Attestation | NewExternalUserTimeoutInHours**: Legen Sie fest, wie viele Stunden der Bestätigungslink für neue externe Benutzer gültig ist.

     Standardmäßig ist der Bestätigungslink 4 Stunden gültig. Wenn die Anmeldung am Kennwortrücksetzungsportal fehl schlägt, weil diese Zeit abgelaufen ist, kann der Benutzer sich einen neuen Bestätigungslink zusenden lassen. Um den Gültigkeitszeitraum des Bestätigungslinks zu ändern, passen Sie den Wert des Konfigurationsparameters an.
   - **QER | Attestation | NewExternalUserFinalTimeoutInHours**: Legen Sie fest, nach wie vielen Stunden die Selbstregistrierung neuer Benutzer abgebrochen wird, sofern die Registrierung noch nicht erfolgreich abgeschlossen wurde.

     Wenn der Benutzer die Registrierung nicht innerhalb von 24 Stunden abgeschlossen hat, wird der Attestierungsvorgang abgebrochen. Um sich dennoch zu registrieren, muss sich der Benutzer erneut vollständig am Web Portal anmelden. Um die Gültigkeitsdauer der Registrierung zu ändern, passen Sie den Wert des Konfigurationsparameters an.
2. Weisen Sie der Anwendungsrolle **Identity & Access Governance | Attestierung | Attestierer für externe Benutzer** mindestens eine Person zu.

### Detaillierte Informationen zum Thema

- Selbstregistrierung neuer Benutzer im Web Portal auf Seite 139
- Anlegen neuer Personen durch einen Manager oder Personenadministrator auf Seite 142
- Importieren neuer Personenstammdaten auf Seite 145
- Ablauf der Rezertifizierung auf Seite 149
- Bestätigungslink für neue externe Benutzer auf Seite 121

# Attestierung neuer Benutzer

Für die Attestierung neuer Benutzer unterscheidet der One Identity Manager drei Anwendungsfälle:

1. Registrieren eines neuen externen Benutzers bei der Anmeldung im Web Portal
2. Anlegen neuer Personen im Manager oder durch einen Manager im Web Portal
3. Anlegen neuer Personen durch Import der Personenstammdaten

Das Ergebnis der Attestierung ist in allen drei Anwendungsfällen identisch.

- Personen, die zertifiziert und aktiviert sind und damit über alle ihnen zugewiesenen Berechtigungen im One Identity Manager und den angeschlossenen Zielsystemen verfügen.

  Unternehmensressourcen werden vererbt. Kontendefinitionen werden an interne Personen zugewiesen.

  - ODER -

- Personen, die abgelehnt und dauerhaft deaktiviert sind.

  Deaktivierte Personen können sich nicht an den One Identity Manager Werkzeugen anmelden. Unternehmensressourcen werden nicht vererbt. Kontendefinitionen werden nicht automatisch zugewiesen. Mit der Person verbundene Benutzerkonten werden gegebenenfalls gesperrt oder gelöscht. Das gewünschte Verhalten können Sie unternehmensspezifisch konfigurieren.

# Selbstregistrierung neuer Benutzer im Web Portal

Noch nicht registrierte Benutzer haben die Möglichkeit sich für die Nutzung des Web Portals selbst zu registrieren. Diese Benutzer können sich am Web Portal anmelden, sobald die verantwortlichen Personen die Stammdaten des Benutzers attestiert haben und die Benutzer ein Kennwort gesetzt haben. In der One Identity Manager-Datenbank wird eine externe Person angelegt.

Ablauf der Attestierung:

1. Der Benutzer meldet sich erstmalig am Web Portal an und erfasst die benötigten Stammdaten.

   Ein neues Personenobjekt wird in der One Identity Manager-Datenbank angelegt mit den Eigenschaften:

   **Tabelle 51: Eigenschaften einer neu angelegten Person**

   | Eigenschaft | Wert |
   |---|---|
   | Zertifizierungsstatus | Neu |
   | Extern | aktiviert |
   | Kontakt-E-Mail-Adresse | E-Mail-Adresse, an die der Bestätigungslink geschickt wird. |
   | Dauerhaft deaktiviert | aktiviert |
   | Keine Vererbung | aktiviert |

2. Die Attestierung startet automatisch.

   Genutzte Attestierungsrichtlinie: **Zertifizierung neuer Benutzer**

   HINWEIS: Die Attestierung startet nur dann automatisch, wenn der Konfigurationsparameter **QER | Attestation | UserApproval** aktiviert ist. Andernfalls bleibt der neue Benutzer dauerhaft deaktiviert, bis ein Verantwortlicher die Personenstammdaten manuell ändert.

3. Die Attestierer werden ermittelt.

   Wirksame Entscheidungsrichtlinie: **Zertifizierung von Benutzern**

4. Wenn der Konfigurationsparameter **QER | Attestation | ApproveNewExternalUsers** aktiviert ist und der Wert **1** eingestellt ist, wird der Attestierungsvorgang den Mitgliedern der Anwendungsrolle **Identity & Access Governance | Attestierung | Attestierer für externe Benutzer** vorgelegt.

   a. Wenn ein Attestierer für externe Benutzer die Attestierung ablehnt, ist der Attestierungsvorgang abgeschlossen. Die Eigenschaften des Personenobjekts werden in der Datenbank aktualisiert.

      **Tabelle 52: Eigenschaften einer externen Person mit abgelehnter Attestierung**

      | Eigenschaft | Wert | Erläuterung |
      |---|---|---|
      | Zertifizierungsstatus | Abgelehnt | |
      | Extern | aktiviert | |

| Eigenschaft | Wert | Erläuterung |
|---|---|---|
| Dauerhaft deaktiviert | aktiviert | Der Benutzer kann sich nicht am Web Portal anmelden. |
| Keine Vererbung | aktiviert | Unternehmensressourcen werden nicht vererbt. |

b. Wenn ein Attestierer für externe Benutzer der Attestierung zustimmt, wird eine E-Mail mit einem Bestätigungslink an den neuen Benutzer versendet.

HINWEIS: Wenn der Konfigurationsparameter **QER | Attestation | ApproveNewExternalUsers** deaktiviert ist oder der Wert **0** eingestellt ist, wird sofort eine E-Mail mit dem Bestätigungslink an den neuen Benutzer versendet.

5. Sobald der Benutzer dem Bestätigungslink gefolgt ist und ein Kennwort sowie die Kennwortfragen festgelegt hat, wird der Attestierungsvorgang genehmigt. Die Eigenschaften des Personenobjekts werden in der Datenbank aktualisiert.

**Tabelle 53: Eigenschaften einer externen Person mit genehmigter Attestierung**

| Eigenschaft | Wert | Erläuterung |
|---|---|---|
| Zertifizierungsstatus | Zertifiziert | |
| Extern | aktiviert | |
| Dauerhaft deaktiviert | deaktiviert | Der Benutzer kann sich am Web Portal anmelden. |
| Keine Vererbung | deaktiviert | Unternehmensressourcen werden vererbt. |

Standardmäßig ist der Bestätigungslink 4 Stunden gültig. Wenn die Anmeldung am Kennwortrücksetzungsportal fehl schlägt, weil diese Zeit abgelaufen ist, kann der Benutzer sich einen neuen Bestätigungslink zusenden lassen.

Wenn der Benutzer die Registrierung nicht innerhalb von 24 Stunden abgeschlossen hat, wird der Attestierungsvorgang abgebrochen. Um sich dennoch zu registrieren, muss sich der Benutzer erneut vollständig am Web Portal anmelden.

## Verwandte Themen

- Attestierung und Rezertifizierung von Benutzern konfigurieren auf Seite 138

# Anlegen neuer Personen durch einen Manager oder Personenadministrator

Eine Attestierung neuer Benutzer ist auch dann möglich, wenn im Manager neue Personen angelegt werden oder wenn ein Manager im Web Portal einen neuen Mitarbeiter hinzufügt. Das gewünschte Verhalten wird am Konfigurationsparameter **QER | Attestation | UserApproval | InitialApprovalState** festgelegt. Standardmäßig hat der Konfigurationsparameter den Wert **0**. Damit erhält jede neue Person den Zertifizierungsstatus **Zertifiziert**. Es wird keine automatische Attestierung durchgeführt.

***Damit neue Benutzer automatisch attestiert werden können***

- Aktivieren Sie im Designer den **Konfigurationsparameter QER | Attestation | UserApproval | InitialApprovalState** und setzen Sie den Wert auf **1**.

  Alle Personen, die ab diesem Zeitpunkt neu in der Datenbank angelegt werden, erhalten den Zertifizierungsstatus **Neu**. Damit wird eine automatische Attestierung dieser Personen durchgeführt.

Für interne und externe Personen gelten jeweils unterschiedliche Abläufe.

Ablauf der Attestierung:

1. Erfassen Sie die Stammdaten des neuen Benutzers und ordnen Sie einen Manager zu.

   Ausführliche Informationen zum Anlegen von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul* und im *One Identity Manager Anwenderhandbuch für das Web Portal*.

   Der Zertifizierungsstatus entspricht dem Wert des Konfigurationsparameters **QER | Attestation | UserApproval | InitialApprovalState**. Wenn am Konfigurationsparameter der Wert **1** gesetzt ist, wird der Zertifizierungsstatus **Neu** gesetzt.

   Die Person ist standardmäßig aktiviert und kann sich sofort am One Identity Manager anmelden.

   - Wenn neue Benutzer sich erst dann am One Identity Manager anmelden dürfen, wenn ihre Stammdaten attestiert wurden, führen Sie die Aufgabe **Person dauerhaft deaktivieren** aus.

2. Sobald die Personenstammdaten gespeichert wurden, startet die Attestierung.

   Genutzte Attestierungsrichtlinie: **Zertifizierung neuer Benutzer**

3. Die Attestierer werden ermittelt.

   Wirksame Entscheidungsrichtlinie: **Zertifizierung von Benutzern**

4. Wenn an der Person die Option **Extern** aktiviert ist:

   Die Attestierung läuft wie im Abschnitt Selbstregistrierung neuer Benutzer im Web Portal, Schritt 4 bis 5 beschrieben ab.

5. Wenn an der Person die Option **Extern** deaktiviert ist:
    a. Der One Identity Manager prüft, ob der Person ein Manager zugeordnet wurde.
        - Wenn der Person ein Manager zugeordnet wurde, wird der Vorgang sofort diesem Manager zur Entscheidung zugewiesen.
        - Wenn der Person kein Manager zugeordnet wurde, wird der Vorgang den Personenadministratoren zur Entscheidung zugewiesen.
    b. Ein Personenadministrator prüft die Stammdaten des neuen Benutzers und ordnet gegebenenfalls einen Manager zu.
        - Ein Personenadministrator ordnet einen Manager zu und stimmt der Attestierung zu. Der Vorgang wird dem Manager zur Entscheidung zugewiesen.
        - Wenn ein Personenadministrator keinen Manager zuordnet und der Attestierung zustimmt, ist der Attestierungsvorgang abgeschlossen. Die Eigenschaften des Personenobjekts werden in der Datenbank aktualisiert.

          **Tabelle 54: Eigenschaften einer Person mit genehmigter Attestierung**

          | Eigenschaft | Wert | Erläuterung |
          |---|---|---|
          | Zertifizierungsstatus | Zertifiziert | |
          | Extern | deaktiviert | |
          | Dauerhaft deaktiviert | deaktiviert | |
          | Keine Vererbung | deaktiviert | Unternehmensressourcen werden vererbt. |

        - Wenn ein Personenadministrator die Attestierung ablehnt, ist der Attestierungsvorgang abgeschlossen. Die Eigenschaften des Personenobjekts werden in der Datenbank aktualisiert.

          **Tabelle 55: Eigenschaften einer Person mit abgelehnter Attestierung**

          | Eigenschaft | Wert | Erläuterung |
          |---|---|---|
          | Zertifizierungsstatus | Abgelehnt | |
          | Extern | deaktiviert | |
          | Dauerhaft deaktiviert | aktiviert | |
          | Keine Vererbung | aktiviert | Unternehmensressourcen werden |

| Eigenschaft | Wert | Erläuterung |
|---|---|---|
| | | nicht vererbt.<br>Benutzerkonten werden nicht automatisch erstellt. |

c. Der Manager kann die Attestierung ablehnen, wenn er nicht der verantwortliche Manager dieses Benutzers ist.
   - Er kann eine andere Person als Manager zuordnen. Diesem wird der Vorgang sofort zur Entscheidung zugewiesen.
   - Wenn ihm der korrekte Manager nicht bekannt ist, wird die Entscheidung an die Personenadministratoren zurückgegeben. Diese können
     - einen anderen Manager zuordnen,
     - keinen neuen Manager zuordnen und der Attestierung zustimmen oder
     - die Attestierung ablehnen.

d. Wenn der Manager der Attestierung zustimmt, ist der Attestierungsvorgang abgeschlossen. Die Eigenschaften des Personenobjekts werden in der Datenbank aktualisiert.

**Tabelle 56: Eigenschaften einer Person mit genehmigter Attestierung**

| Eigenschaft | Wert | Erläuterung |
|---|---|---|
| Zertifizierungsstatus | Zertifiziert | |
| Extern | deaktiviert | |
| Dauerhaft deaktiviert | deaktiviert | |
| Keine Vererbung | deaktiviert | Unternehmensressourcen werden vererbt. |

HINWEIS: Die Attestierung endgültig ablehnen können nur die Personenadministratoren. Wenn ein Manager die Attestierung ablehnt, wird der Vorgang in jedem Fall an die Personenadministratoren zur Entscheidung zurückgewiesen.

## Verwandte Themen

- Attestierung und Rezertifizierung von Benutzern konfigurieren auf Seite 138

# Importieren neuer Personenstammdaten

Eine Attestierung neuer Personen kann angefordert werden, wenn die Personenstammdaten aus anderen Systemen in die One Identity Manager-Datenbank importiert werden. Damit neue Personen automatisch attestiert werden, muss der Zertifizierungsstatus der Person beim Anlegen auf **Neu** gesetzt werden (`Person.ApprovalState='1'`). Dafür gibt es zwei Möglichkeiten:

1. Für den Zertifizierungsstatus wird der Konfigurationsparameter **QER | Attestation | UserApproval | InitialApprovalState** ausgewertet. Wenn am Konfigurationsparameter der Wert **1** gesetzt ist, wird der Zertifizierungsstatus **Neu** gesetzt.

   Voraussetzung: Der Import verändert nicht die Eigenschaft `Person.ApprovalState`.

   > HINWEIS: Standardmäßig hat der Konfigurationsparameter **QER | Attestation | UserApproval | InitialApprovalState**den Wert **0**. Damit erhält jede neue Person den Zertifizierungsstatus **Zertifiziert**. Es wird keine automatische Attestierung durchgeführt.
   >
   > Wenn neue Personen sofort attestiert werden sollen, ändern Sie den Wert des Konfigurationsparameters auf **1**.

2. Der Import setzt explizit die Eigenschaft `Person.ApprovalState`.
   - Der Import setzt `ApprovalState='1'` (**Neu**).

     Die Person wird automatisch durch ihren Manager attestiert.
   - Der Import setzt `ApprovalState='0'` (**Zertifiziert**).

     Die importierten Personenstammdaten sind bereits authorisiert. Sie sollen nicht erneut attestiert werden.
   - Der Import setzt `ApprovalState='3'` (**Abgelehnt**).

     Die Person wird dauerhaft deaktiviert und nicht attestiert.

Die Attestierung neuer Benutzer wird ausgelöst, wenn

- der Konfigurationsparamter **QER | Attestation | UserApproval** aktiviert ist,
- neue Personenstammdaten in die One Identity Manager-Datenbank importiert wurden,
- der Zertifizierungsstatus der neuen Personen **Neu** ist und
- keine **Datenquelle Import** an der Person hinterlegt ist.

Wenn an der Person die Option **Extern** deaktiviert ist, läuft die Attestierung wie im Abschnitt Anlegen neuer Personen durch einen Manager oder Personenadministrator, Schritt 5 beschrieben ab.

Wenn an der Person die Option **Extern** aktiviert ist, läuft die Attestierung wie im Abschnitt Selbstregistrierung neuer Benutzer im Web Portal, Schritt 4 bis 5 beschrieben ab.

Es wird die Attestierungsrichtlinie **Zertifizierung neuer Benutzer** ausgeführt.

### Verwandte Themen

- Attestierung und Rezertifizierung von Benutzern konfigurieren auf Seite 138

# Zeitgesteuerte Attestierungen

Benutzer werden auch dann attestiert, wenn der Zertifizierungsstatus einer Person nachträglich (manuell oder per Import) auf **Neu** gesetzt wird. Dafür ist der Attestierungsrichtlinie **Zertifizierung neuer Benutzer** der Zeitplan **Daily** zugeordnet. Die Attestierung neuer Benutzer wird ausgelöst, wenn der in diesem Zeitplan angegebene Ausführungszeitpunkt erreicht ist. Dabei werden alle Personen ermittelt, deren Zertifizierungsstatus **Neu** ist und für die es keinen offenen Attestierungsvorgang gibt.

Sie können der Attestierungsrichtlinie bei Bedarf einen unternehmensspezifischen Zeitplan zuweisen.

### Detaillierte Informationen zum Thema

- Zeitpläne auf Seite 19

# Einschränken der Attestierungsobjekte für die Zertifizierung

> WICHTIG: Für unternehmensspezifische Anpassungen der Standardattestierung **Zertifizierung neuer Benutzer** sind Änderungen an One Identity Manager-Objekten erforderlich. Nutzen Sie für diese Änderungen immer eine unternehmensspezifische Kopie des jeweiligen Objekts!

Es kann notwendig sein, die Attestierung neuer Benutzer auf bestimmte Personengruppen einzuschränken, beispielsweise wenn nur neue Mitarbeiter einer bestimmten Abteilung attestiert werden sollen. Dafür können Sie die Bedingung an der Attestierungsrichtlinie erweitern. Erstellen Sie dafür eine unternehmensspezifische Attestierungsrichtlinie.

Damit die Attestierung neuer Benutzer mit dieser Attestierungsrichtlinie durchgeführt werden kann, müssen folgende Objekte angepasst werden. Erstellen Sie dafür immer eine Kopie des jeweiligen Objekts.

- Attestierungsrichtlinie **Zertifizierung neuer Benutzer**
- Prozess `VI_Attestation_Person_new_AttestationCase_for_Certification`
- Prozess `VI_Attestation_AttestationCase_Person_Approval_Granted`
- Prozess `VI_Attestation_AttestationCase_Person_Approval_Dismissed`

WICHTIG: Damit die Attestierung im Web Portal fehlerfrei durchgeführt werden kann, müssen der Attestierungsrichtlinie das Standard-Attestierungsverfahren **Zertifizierung von Benutzern** und die Standard-Entscheidungsrichtlinie **Zertifizierung von Benutzern** zugeordnet sein.

Das Standard-Attestierungsverfahren, die Standard-Entscheidungsrichtlinie und der Standard-Entscheidungsworkflow **Zertifizierung von Benutzern** dürfen nicht verändert werden.

***Um die standardmäßige Attestierung neuer Benutzer unternehmensspezifisch anzupassen***

1. Kopieren Sie die Attestierungsrichtlinie **Zertifizierung neuer Benutzer** und passen Sie die Kopie an.

   **Tabelle 57: Eigenschaften der Attestierungsrichtlinie**

   | Eigenschaft | Wert |
   |---|---|
   | Attestierungsverfahren | Zertifizierung von Benutzern |
   | Entscheidungsrichtlinie | Zertifizierung von Benutzern |
   | Bedingung bearbeiten | Die Standardbedingung muss unverändert übernommen werden, damit die korrekten Attestierungsobjekte ausgewählt werden.<br>Um die Menge der Attestierungsobjekte einzuschränken, kann die Datenbankabfrage um zusätzliche Teilbedingungen erweitert werden. |

2. Kopieren Sie im Designer den Prozess `VI_Attestation_Person_new_AttestationCase_for_Certification` des Basisobjekts `Person` und passen Sie die Kopie an.

   **Tabelle 58: Prozesseigenschaften mit Änderungen**

   | Prozessschritt | Parameter | Änderung |
   |---|---|---|
   | `Create attestation instance` | `WhereClause` | Ersetzen Sie die UID der Attestierungsrichtlinie **Zertifizierung neuer Benutzer** durch die UID der neuen Attestierungsrichtlinie. |

3. Kopieren Sie im Designer den Prozess `VI_Attestation_AttestationCase_Person_Approval_Granted` des Basisobjekts `AttestationCase` und passen Sie die Kopie an.

   **Tabelle 59: Prozesseigenschaften mit Änderungen**

   | Prozesseigenschaft | Änderung |
   |---|---|
   | Prä-Skript zur Generierung | Ersetzen Sie die UID der Attestierungsrichtlinie **Zertifizierung neuer Benutzer** durch die UID der |

| Prozesseigenschaft | Änderung |
|---|---|
| Generierungsbedingung | neuen Attestierungsrichtlinie. |

4. Kopieren Sie im Designer den Prozess `VI_Attestation_AttestationCase_Person_Approval_Dismissed` des Basisobjekts `AttestationCase` und passen Sie die Kopie an.

   **Tabelle 60: Prozesseigenschaften mit Änderungen**

| Prozesseigenschaft | Änderung |
|---|---|
| Prä-Skript zur Generierung | Ersetzen Sie die UID der Attestierungsrichtlinie **Zertifizierung neuer Benutzer** durch die UID der neuen Attestierungsrichtlinie. |
| Generierungsbedingung | |

Ausführliche Informationen zum Bearbeiten von Prozessen finden Sie im *One Identity Manager Konfigurationshandbuch*.

### Detaillierte Informationen zum Thema

- Allgemeine Stammdaten von Attestierungsrichtlinien auf Seite 28
- Kopie erstellen auf Seite 36

# Rezertifizierung vorhandener Benutzer

WICHTIG: Als Ergebnis der Rezertifizierung wird One Identity Manager Benutzern möglicherweise der Zugang zu den angeschlossenen Zielsystemen entzogen. Das Verhalten können Sie unternehmensspezifisch konfigurieren. Lesen Sie den folgenden Abschnitt aufmerksam durch, bevor Sie die Rezertifizierungsfunktion nutzen.

Damit Unternehmen die im One Identity Manager gespeicherten Personenstammdaten regelmäßig überprüfen und autorisieren können, stellt der One Identity Manager eine Attestierungsrichtlinie zur zyklischen Attestierung vorhandener Benutzer bereit. Die zyklische Attestierung wird durch einen zeitgesteuerten Auftrag ausgelöst. Dabei wird der Zertifizierungsstatus für alle in der Datenbank gespeicherten Personen neu gesetzt. Der One Identity Manager nutzt dafür das selbe Verfahren wie für die Attestierung neuer Benutzer. Der Vorgang wird als Rezertifizierung bezeichnet.

### Ergebnis der Rezertifizierung

- Personen, die zertifiziert und aktiviert sind und damit über alle ihnen zugewiesenen Berechtigungen im One Identity Manager und den angeschlossenen Zielsystemen verfügen.

Unternehmensressourcen werden vererbt. Kontendefinitionen werden an interne Personen zugewiesen.

- ODER -

- Personen, die abgelehnt und dauerhaft deaktiviert sind.

  Deaktivierte Personen können sich nicht an den One Identity Manager Werkzeugen anmelden. Unternehmensressourcen werden nicht vererbt. Kontendefinitionen werden nicht automatisch zugewiesen. Mit der Person verbundene Benutzerkonten werden gegebenenfalls gesperrt oder gelöscht. Das gewünschte Verhalten können Sie unternehmensspezifisch konfigurieren.

# Rezertifizierung vorbereiten

***Um die regelmäßige Attestierung von Benutzern einzurichten***

1. Aktivieren Sie im Designer die benötigten Konfigurationsparameter.
2. Erstellen Sie einen Zeitplan und ordnen Sie diesen der Attestierungsrichtlinie **Rezertifizierung von Benutzern** zu. Dabei ersetzen Sie den standardmäßig zugeordneten Zeitplan.
   - Aktivieren Sie den Zeitplan.

### Detaillierte Informationen zum Thema

- Attestierung und Rezertifizierung von Benutzern konfigurieren auf Seite 138

### Verwandte Themen

- Allgemeine Stammdaten von Attestierungsrichtlinien auf Seite 28
- Zeitpläne auf Seite 19

# Ablauf der Rezertifizierung

Für die Rezertifizierung nutzt der One Identity Manager dasselbe Verfahren, wie für die Zertifizierung neuer Benutzer. Die Rezertifizierung von Benutzern wird ausgelöst, wenn

- der Konfigurationsparamter **QER | Attestation | UserApproval** aktiviert ist,
- keine **Datenquelle Import** an der Person hinterlegt ist oder die **Datenquelle Import** nicht **E-Business Suite** ist und
- der Ausführungszeitpunkt des an der Attestierungsrichtlinie **Rezertifizierung von Benutzern** hinterlegten Zeitplans erreicht ist.

Interne Personen werden durch ihre Manager attestiert. Wenn einer Person kein Manager zugeordnet ist, ordnet zuerst ein Personenadministrator einen Manager zu. Die Rezertifizierung endgültig ablehnen können nur die Personenadministratoren. Wenn ein

Manager die Rezertifizierung ablehnt, wird der Vorgang in jedem Fall an die Personenadministratoren zur Entscheidung zurückgewiesen.

Externe Personen werden durch die Mitglieder der Anwendungsrolle **Identity & Access Governance | Attestierung | Attestierer für externe Benutzer** attestiert.

Wenn an der Person die Option **Extern** deaktiviert ist, läuft die Attestierung wie im Abschnitt Anlegen neuer Personen durch einen Manager oder Personenadministrator, Schritt 5 beschrieben ab.

Wenn an der Person die Option **Extern** aktiviert ist, läuft die Attestierung wie im Abschnitt Selbstregistrierung neuer Benutzer im Web Portal, Schritt 4 bis 5 beschrieben ab.

Die Attestierer werden über die Entscheidungsrichtlinie **Zertifizierung von Benutzern** ermittelt.

# Einschränken der Attestierungsobjekte für die Rezertifizierung

WICHTIG: Für unternehmensspezifische Anpassungen der Standardattestierung **Rezertifizierung von Benutzern** sind Änderungen an One Identity Manager-Objekten erforderlich. Nutzen Sie für diese Änderungen immer eine unternehmensspezifische Kopie des jeweiligen Objekts.

Über die im One Identity Manager bereitgestellte Attestierungsrichtlinie **Rezertifizierung von Benutzern** werden alle in der Datenbank gespeicherten Personen rezertifiziert. Es kann notwendig sein, die Rezertifizierung von Benutzern auf bestimmte Personengruppen einzuschränken, beispielsweise wenn nur die Mitarbeiter einer bestimmten Abteilung rezertifiziert werden sollen. Dafür können Sie die Bedingung an der Attestierungsrichtlinie erweitern. Erstellen Sie dafür eine unternehmensspezifische Attestierungsrichtlinie.

Damit die Rezertifizierung von Benutzern mit dieser Attestierungsrichtlinie durch geführt werden kann, müssen folgende Objekte angepasst werden. Erstellen Sie dafür immer eine Kopie des jeweiligen Objekts.

- Attestierungsrichtlinie **Rezertifizierung von Benutzern**
- Prozess `VI_Attestation_AttestationCase_Person_Approval_Granted`
- Prozess `VI_Attestation_AttestationCase_Person_Approval_Dismissed`

WICHTIG: Damit die Rezertifizierung im Web Portal fehlerfrei durchgeführt werden kann, müssen der Attestierungsrichtlinie das Standard-Attestierungsverfahren **Zertifizierung von Benutzern** und die Standard-Entscheidungsrichtlinie **Zertifizierung von Benutzern** zugeordnet sein.

Das Standard-Attestierungsverfahren, die Standard-Entscheidungsrichtlinie und der Standard-Entscheidungsworkflow **Zertifizierung von Benutzern** dürfen nicht verändert werden.

***Um die standardmäßige Rezertifizierung von Benutzern unternehmensspezifisch anzupassen***

1. Kopieren Sie die Attestierungsrichtlinie **Rezertifizierung von Benutzern** und passen Sie die Kopie an.

   **Tabelle 61: Eigenschaften der Attestierungsrichtlinie**

   | Eigenschaft | Wert |
   |---|---|
   | Attestierungsverfahren | Zertifizierung von Benutzern |
   | Entscheidungsrichtlinie | Zertifizierung von Benutzern |
   | Bedingung bearbeiten | Die Standardbedingung muss unverändert übernommen werden, damit die korrekten Attestierungsobjekte ausgewählt werden.<br>Um die Menge der Attestierungsobjekte einzuschränken, kann die Datenbankabfrage um zusätzliche Teilbedingungen erweitert werden. |

2. Kopieren Sie im Designer den Prozess `VI_Attestation_AttestationCase_Person_Approval_Granted` des Basisobjekts `AttestationCase` und passen Sie die Kopie an.

   **Tabelle 62: Prozesseigenschaften mit Änderungen**

   | Prozesseigenschaft | Änderung |
   |---|---|
   | Prä-Skript zur Generierung | Ersetzen Sie die UID der Attestierungsrichtlinie **Rezertifizierung von Benutzern** durch die UID der neuen Attestierungsrichtlinie. |
   | Generierungsbedingung | |

3. Kopieren Sie im Designer den Prozess `VI_Attestation_AttestationCase_Person_Approval_Dismissed` des Basisobjekts `AttestationCase` und passen Sie die Kopie an.

   **Tabelle 63: Prozesseigenschaften mit Änderungen**

   | Prozesseigenschaft | Änderung |
   |---|---|
   | Prä-Skript zur Generierung | Ersetzen Sie die UID der Attestierungsrichtlinie **Rezertifizierung von Benutzern** durch die UID der neuen Attestierungsrichtlinie. |
   | Generierungsbedingung | |

Ausführliche Informationen zum Bearbeiten von Prozessen finden Sie im *One Identity Manager Konfigurationshandbuch*.

### Detaillierte Informationen zum Thema

- Allgemeine Stammdaten von Attestierungsrichtlinien auf Seite 28
- Kopie erstellen auf Seite 36

# 6

# Risikomindernde Maßnahmen

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

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

Risikomindernde Maßnahmen beschreiben Maßnahmen, die umgesetzt werden sollen, wenn eine Attestierung abgelehnt wurde. Nach Umsetzung der Maßnahmen sollte die Attestierung im nächsten Attestierungslauf genehmigt werden können.

***Um risikomindernde Maßnahmen zu bearbeiten***

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

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

# Allgemeine Stammdaten von risikomindernden Maßnahmen

***Um risikomindernde Maßnahmen zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **Risikoindex-Berechnungsvorschriften | Risikomindernde Maßnahmen**.
2. Wählen Sie in der Ergebnisliste eine risikomindernde Maßnahme und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

   Klicken Sie in der Ergebnisliste .

3. Bearbeiten Sie die Stammdaten der risikomindernden Maßnahme.
4. Speichern Sie die Änderungen.

Für eine risikomindernde Maßnahme erfassen Sie folgende Stammdaten.

**Tabelle 64: Allgemeine Stammdaten einer risikomindernden Maßnahme**

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

# Zusätzliche Aufgaben für risikomindernde Maßnahmen

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

# Überblick über die risikomindernde Maßnahme

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

***Um einen Überblick über eine risikomindernde Maßnahme zu erhalten***

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

# Attestierungsrichtlinien zuweisen

Mit dieser Aufgabe legen Sie fest, für welche Attestierungsrichtlinien eine risikomindernde Maßnahme gilt.

***Um Attestierungsrichtlinien 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 **Attestierungsrichtlinien zuweisen**.

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

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

   ***Um eine Zuweisung zu entfernen***

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

# Risikominderung berechnen

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

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

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

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

# Anhang: Konfigurationsparameter für die Attestierung

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

**Tabelle 65: Übersicht der Konfigurationsparameter**

| Konfigurationsparameter | Beschreibung |
|---|---|
| QER \| Attestation | Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Attestierung. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren.<br>Ist der Parameter aktiviert, können Sie die Attestierungsfunktion nutzen. |
| QER \| Attestation \| AllowAllReportTypes | Der Konfigurationsparameter legt fest, ob für Attestierungsrichtlinien alle Berichtsformate erlaubt sind. Standardmäßig ist nur PDF erlaubt, da dies als einziges Format revisionssicher ist. |
| QER \| Attestation \| ApproveNewExternalUsers | Der Konfigurationsparameter legt fest, ob neue externe Benutzer attestiert werden müssen, bevor sie aktiviert werden. |
| QER \| Attestation \| AutoCloseInactivePerson | Ist der Konfigurationsparameter aktiviert, werden offene Attestierungsvorgänge für eine Person geschlossen, sobald die Person dauerhaft deaktiviert wird. |
| QER \| Attestation \| AutoRemovalScope | Allgemeiner Konfigurationsparameter zur Definition des automatischen Entzugs von Berechtigungen nach einer negativen Entscheidung im Rahmen einer Attestierung. |
| QER \| Attestation \| | Bestimmt das Standardverhalten für das |

| Konfigurationsparameter | Beschreibung |
|---|---|
| AutoRemovalScope \| AERoleMembership | Entfernen von Mitgliedschaften in Anwendungsrollen bei negativer Attestierung. |
| QER \| Attestation \| AutoRemovalScope \| AERoleMembership \| RemoveDelegatedRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Delegierung der Anwendungsrolle beendet. |
| QER \| Attestation \| AutoRemovalScope \| AERoleMembership \| RemoveDirectRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Mitgliedschaft der Person in der Anwendungsrolle entfernt. |
| QER \| Attestation \| AutoRemovalScope \| AERoleMembership \| RemoveRequestedRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Bestellung der Mitgliedschaft in der Anwendungsrolle abgebrochen. |
| QER \| Attestation \| AutoRemovalScope \| DepartmentHasESet | Bestimmt das Standardverhalten für das Entfernen von Zuweisungen von Systemrollen an Abteilungen bei negativer Attestierung. |
| QER \| Attestation \| AutoRemovalScope \| DepartmentHasESet \| RemoveDirect | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuweisung der Systemrolle an die Abteilung entfernt. |
| QER \| Attestation \| AutoRemovalScope \| DepartmentHasUNSGroup | Bestimmt das Standardverhalten für das Entfernen von Zuweisungen von Systemberechtigungen an Abteilungen bei negativer Attestierung. |
| QER \| Attestation \| AutoRemovalScope \| DepartmentHasUNSGroup \| RemoveDirect | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuweisung der Systemberechtigung an die Abteilung entfernt. |
| QER \| Attestation \| AutoRemovalScope \| ESetAssignment | Bestimmt das Standardverhalten für das Entfernen von Mitgliedschaften in Systemrollen bei negativer Attestierung. |
| QER \| Attestation \| AutoRemovalScope \| ESetAssignment \| RemoveDelegatedRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Delegierung der Rolle beendet, über welche die Person die Systemrolle erhalten hat.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Rolle erhalten hat! |
| QER \| Attestation \| AutoRemovalScope \| | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die direkte Mitglied- |

| Konfigurationsparameter | Beschreibung |
| --- | --- |
| ESetAssignment \| RemoveDirect | schaft in der Systemrolle entfernt.<br>Damit werden alle indirekten Zuweisungen, welche die Person über die Systemrolle erhalten hat, entfernt! |
| QER \| Attestation \| AutoRemovalScope \| ESetAssignment \| RemoveDirectRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuweisung der Systemrolle an Rollen (Organisationen und Geschäftsrollen) entfernt. Damit wird die Zuweisung der Systemrolle zu allen Personen entfernt, die Mitglied dieser Rollen sind.<br>WICHTIG: Dadurch können auch Personen die Systemrolle verlieren, deren Attestierung genehmigt wurde! |
| QER \| Attestation \| AutoRemovalScope \| ESetAssignment \| RemovePrimaryRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuordnung der primären Rolle, über welche die Person die Systemrolle erhalten hat, von der Person entfernt.<br>Damit werden alle indirekten Zuweisungen, welche die Person über diese Rolle erhalten hat, entfernt! |
| QER \| Attestation \| AutoRemovalScope \| ESetAssignment \| RemoveRequested | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die bestellte Systemrolle abbestellt.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über die Systemrolle erhalten hat! |
| QER \| Attestation \| AutoRemovalScope \| ESetAssignment \| RemoveRequestedRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Bestellung der Rolle abgebrochen, über welche die Person die Systemrolle erhalten hat.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Rolle erhalten hat! |
| QER \| Attestation \| AutoRemovalScope \| ESetHasEntitlement | Bestimmt das Standardverhalten für das Entfernen von Zuweisungen an Systemrollen bei negativer Attestierung. |
| QER \| Attestation \| AutoRemovalScope \| ESetHasEntitlement \| RemoveDirect | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuweisung der |

| Konfigurationsparameter | Beschreibung |
|---|---|
| | Unternehmensressource an eine Systemrolle entfernt. |
| QER \| Attestation \| AutoRemovalScope \| GroupMembership | Bestimmt das Standardverhalten für das Entfernen von Mitgliedschaften in Unified Namespace Systemberechtigungen bei negativer Attestierung. |
| QER \| Attestation \| AutoRemovalScope \| GroupMembership \| RemoveDelegatedRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Delegierung der Rolle beendet, über welche die Person die Systemberechtigung erhalten hat.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Rolle erhalten hat! |
| QER \| Attestation \| AutoRemovalScope \| GroupMembership \| RemoveDirect | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die direkte Mitgliedschaft des Benutzerkontos in der Systemberechtigung entfernt. |
| QER \| Attestation \| AutoRemovalScope \| GroupMembership \| RemoveDirectRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuweisung der Systemberechtigung an Rollen (Organisationen und Geschäftsrollen) entfernt. Damit wird die Zuweisung der Systemberechtigung zu allen Benutzerkonten entfernt, deren verbundene Personen Mitglied dieser Rollen sind.<br>WICHTIG: Dadurch können auch Benutzerkonten die Systemberechtigung verlieren, deren Attestierung genehmigt wurde! |
| QER \| Attestation \| AutoRemovalScope \| GroupMembership \| RemovePrimaryRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuordnung der primären Rolle, über welche die Person die Systemberechtigung erhalten hat, von der Person entfernt.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Rolle erhalten hat! |
| QER \| Attestation \| AutoRemovalScope \| GroupMembership \| RemoveRequested | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die bestellte Systemberechtigung abbestellt. |

| Konfigurationsparameter | Beschreibung |
| --- | --- |
| QER \| Attestation \| AutoRemovalScope \| GroupMembership \| RemoveRequestedRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Bestellung der Rolle abgebrochen, über welche die Person die Systemberechtigung erhalten hat.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Rolle erhalten hat! |
| QER \| Attestation \| AutoRemovalScope \| GroupMembership \| RemoveSystemRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuordnung der Systemrolle, über welche die Person die Systemberechtigung erhalten hat, von der Person entfernt.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Systemrolle erhalten hat!<br>HINWEIS: Dieser Konfigurationsparameter ist nur verfügbar, wenn das Systemrollenmodul installiert ist. |
| QER \| Attestation \| AutoRemovalScope \| LocalityHasESet | Bestimmt das Standardverhalten für das Entfernen von Zuweisungen von Systemrollen an Standorte bei negativer Attestierung. |
| QER \| Attestation \| AutoRemovalScope \| LocalityHasESet \| RemoveDirect | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuweisung der Systemrolle an den Standort entfernt. |
| QER \| Attestation \| AutoRemovalScope \| LocalityHasUNSGroup | Bestimmt das Standardverhalten für das Entfernen von Zuweisungen von Systemberechtigungen an Standorte bei negativer Attestierung. |
| QER \| Attestation \| AutoRemovalScope \| LocalityHasUNSGroup \| RemoveDirect | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuweisung der Systemberechtigung an den Standort entfernt. |
| QER \| Attestation \| AutoRemovalScope \| OrgHasESet | Bestimmt das Standardverhalten für das Entfernen von Zuweisungen von Systemrollen an Geschäftsrollen bei negativer Attestierung. |
| QER \| Attestation \| AutoRemovalScope \| OrgHasESet \| RemoveDirect | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuweisung der Systemrolle an die Geschäftsrolle entfernt. |
| QER \| Attestation \| AutoRemovalScope \| OrgHasUNSGroup | Bestimmt das Standardverhalten für das Entfernen von Zuweisungen von System- |

| Konfigurationsparameter | Beschreibung |
| --- | --- |
| | berechtigungen an Geschäftsrollen bei negativer Attestierung. |
| QER \| Attestation \| AutoRemovalScope \| OrgHasUNSGroup \| RemoveDirect | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuweisung der Systemberechtigung an die Geschäftsrolle entfernt. |
| QER \| Attestation \| AutoRemovalScope \| ProfitCenterHasESet | Bestimmt das Standardverhalten für das Entfernen von Zuweisungen von Systemrollen an Kostenstellen bei negativer Attestierung. |
| QER \| Attestation \| AutoRemovalScope \| ProfitCenterHasESet \| RemoveDirect | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuweisung der Systemrolle an die Kostenstelle entfernt. |
| QER \| Attestation \| AutoRemovalScope \| ProfitCenterHasUNSGroup | Bestimmt das Standardverhalten für das Entfernen von Zuweisungen von Systemberechtigungen an Kostenstellen bei negativer Attestierung. |
| QER \| Attestation \| AutoRemovalScope \| ProfitCenterHasUNSGroup \| RemoveDirect | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuweisung der Systemberechtigung an die Kostenstelle entfernt. |
| QER \| Attestation \| AutoRemovalScope \| PWOMethodName | Methode, die auf Bestellungen ausgeführt wird, wenn bei einer negativen Attestierung die bestellte Zuweisung entfernt werden soll.<br>Die Bestellungen können abbestellt (Wert **Unsubscribe**) oder abgebrochen (Wert **Abort**) werden. Wenn der Konfigurationsparameter deaktiviert ist, werden die Bestellungen standardmäßig abgebrochen. |
| QER \| Attestation \| AutoRemovalScope \| RoleMembership | Bestimmt das Standardverhalten für das Entfernen von Mitgliedschaften in Geschäftsrollen bei negativer Attestierung. |
| QER \| Attestation \| AutoRemovalScope \| RoleMembership \| RemoveDelegatedRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Delegierung der Geschäftsrolle beendet.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Geschäftsrolle erhalten hat! |
| QER \| Attestation \| AutoRemovalScope \| RoleMembership \| RemoveDirectRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die sekundäre Mitgliedschaft der Person in der Geschäftsrolle entfernt. |

| Konfigurationsparameter | Beschreibung |
|---|---|
| | Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Geschäftsrolle erhalten hat! |
| QER \| Attestation \| AutoRemovalScope \| RoleMembership \| RemoveRequestedRole | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Bestellung der Mitgliedschaft in der Geschäftsrolle abgebrochen.<br>Damit werden alle indirekten Zuweisungen entfernt, welche die Person über diese Geschäftsrolle erhalten hat! |
| QER \| Attestation \| AutoRemovalScope \| UNSGroupInUNSGroup | Bestimmt das Standardverhalten für das Entfernen von Zuweisungen von Unified Namespace Systemberechtigungen an Systemberechtigungen bei negativer Attestierung. |
| QER \| Attestation \| AutoRemovalScope \| UNSGroupInUNSGroup \| RemoveDirect | Ist der Konfigurationsparameter aktiviert, wird bei negativer Attestierung die Zuweisung der Systemberechtigung an eine Systemberechtigung entfernt. |
| QER \| Attestation \| DefaultSenderAddress | Der Konfigurationsparameter enthält die Absender E-Mail Adresse für automatisch generierte Benachrichtigungen für die Attestierung. |
| QER \| Attestation \| MailApproval \| Account | Name des Benutzerkontos zur Authentifizierung am Postfach, das für die Attestierung per E-Mail genutzt wird. |
| QER \| Attestation \| MailApproval \| DeleteMode | Gibt die Art und Weise an, wie E-Mails im Posteingang gelöscht werden sollen. |
| QER \| Attestation \| MailApproval \| Domain | Domäne des Benutzerkontos zur Authentifizierung am Postfach, das für die Attestierung per E-Mail genutzt wird. |
| QER \| Attestation \| MailApproval \| ExchangeURI | Angabe der Microsoft Exchange Web Service URL. Ist diese nicht spezifiziert, wird der AutoDiscover Modus zur Erkennung der URL verwendet. |
| QER \| Attestation \| MailApproval \| Inbox | Microsoft Exchange Postfach, an das Entscheidungsmails für die Attestierung per E-Mail gesendet werden. |
| QER \| Attestation \| MailApproval \| Password | Kennwort des Benutzerkontos zur Authentifizierung am Postfach, das für die Attestierung per E-Mail genutzt wird. |
| QER \| Attestation \| | Mailvorlage, die genutzt wird, um eine Benach- |

| Konfigurationsparameter | Beschreibung |
|---|---|
| MailTemplateIdents \| AnswerToApprover | richtigung mit der Antwort auf seine Frage an einen Entscheider zu versenden. |
| QER \| Attestation \| MailTemplateIdents \| AttestationApproval | Mailvorlage, die für die Attestierung per E-Mail genutzt wird. |
| QER \| Attestation \| MailTemplateIdents \| InformAddingPerson | Mailvorlage, die genutzt wird, um eine Benachrichtigungs-Mail an einen Entscheider zu versenden, dass sein zusätzlich eingefügter Schritt entschieden wurde. |
| QER \| Attestation \| MailTemplateIdents \| InformDelegatingPerson | Mailvorlage, die genutzt wird, um eine Benachrichtigungs-Mail an einen Entscheider zu versenden, das sein delegierter Schritt entschieden wurde. |
| QER \| Attestation \| MailTemplateIdents \| NewExternalUserVerification | Mailvorlage, die genutzt wird, um eine Benachrichtigung mit einem Bestätigungslink an einen neuen externen Benutzer zu versenden. |
| QER \| Attestation \| MailTemplateIdents \| QueryFromApprover | Mailvorlage, die genutzt wird, um eine Benachrichtigung mit der Frage eines Entscheiders an eine Person zu versenden. |
| QER \| Attestation \| MailTemplateIdents \| RequestApproverByCollection | Mailvorlage, die genutzt wird, um eine Benachrichtigung an einen Entscheider zu versenden, dass noch offene Attestierungen vorliegen. Wenn der Konfigurationsparameter nicht aktiviert ist, kann für einzelne Entscheidungsschritte eine **Mailvorlage Aufforderung** beziehungsweise **Mailvorlage Erinnerung** angegeben werden, welche für jeden einzelnen Attestierungsvorgang versendet wird. Wenn der Konfigurationsparameter aktiviert ist, werden keine Einzelbenachrichtigungen versendet. |
| QER \| Attestation \| NewExternalUserFinalTimeoutInHours | Dauer in Stunden, nach welcher die Registrierung von neuen externen Benutzern endgültig abgebrochen wird (Standard: 24). |
| QER \| Attestation \| NewExternalUserTimeoutInHours | Dauer in Stunden, für die der Zugangscode und der Bestätigungslink für neue externe Benutzer gültig sind (Standard: 4). |
| QER \| Attestation \| OnWorkflowAssign | Der Konfigurationsparameter gibt an, wie offene Attestierungsvorgänge behandelt werden, wenn an der Entscheidungsrichtlinie ein neuer Entscheidungsworkflow zugewiesen wird. |

| Konfigurationsparameter | Beschreibung |
|---|---|
| QER \| Attestation \| OnWorkflowUpdate | Der Konfigurationsparameter gibt an, wie offene Attestierungsvorgänge bei Änderungen am Entscheidungsworkflow behandelt werden. |
| QER \| Attestation \| PersonToAttestNoDecide | Der Konfigurationsparameter legt fest, ob Personen, die attestiert werden, diesen Attestierungsvorgang entscheiden dürfen. Ist der Parameter aktiviert, darf ein Attestierungsvorgang nicht von den Personen entschieden werden, die im Attestierungsobjekt (`AttestationCase.ObjectKeyBase`) oder in den Objektbeziehungen 1-3 (`AttestationCase.UID_ObjectKey1`, `ObjectKey2` oder `ObjectKey3`) enthalten sind. Ist der Parameter nicht aktiviert, dürfen diese Personen über diesen Attestierungsvorgang entscheiden. |
| QER \| Attestation \| ReducedApproverCalculation | Der Konfigurationsparameter legt fest, welche Entscheidungsschritte neu berechnet werden sollen, wenn durch Änderungen von Verantwortlichkeiten die Attestierer neu ermittelt werden müssen. |
| QER \| Attestation \| UserApproval | Attestierungsverfahren zur regelmäßigen Überprüfung und Bestätigung von One Identity Manager Benutzern durch deren Manager werden unterstützt. |
| QER \| Attestation \| UserApproval \| InitialApprovalState | Zertifizierungsstatus für neue Personen. Wird eine Person mit dem Zertifizierungsstatus 1=Neu angelegt, wird eine Attestierung der Daten durch den Manager der Person ausgelöst. |
| QER \| CalculateRiskIndex | Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Berechnung des Risikoindex. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren.<br>Ist der Parameter aktiviert, können Werte für den Risikoindex erfasst und berechnet werden. |
| QER \| Person \| Defender | Der Konfigurationsparameter legt fest, ob die Starling Two-Factor Authentication Integration unterstützt wird. |
| QER \| Person \| Defender \| ApiEndpoint | Der Konfigurationsparameter enthält die URL des Starling 2FA API Endpunktes, über den neue Benutzer registriert werden. |

| Konfigurationsparameter | Beschreibung |
|---|---|
| QER \| Person \| Defender \| ApiKey | Der Konfigurationsparameter enthält den Abonnementschlüssel Ihres Unternehmens zum Zugriff auf die Starling Two-Factor Authentication Schnittstelle. |
| QER \| Person \| Defender \| DisableForceParameter | Der Konfigurationsparameter legt fest, ob Starling 2FA gezwungen werden soll, den Sicherheitscode per SMS oder Telefonanruf zu senden, wenn für die Multifaktor-Authentifizierung eine dieser Optionen ausgewählt ist. Wenn der Konfigurationsparameter aktiviert ist, kann Starling 2FA diese Anforderung zurückweisen; der Benutzer muss dann den Sicherheitscode über die Starling 2FA App anfordern. |
| QER \| WebPortal \| BaseURL | URL zum Web Portal. Diese Adresse wird in Mailvorlagen genutzt, um Hyperlinks auf das Web Portal einzufügen. |
| QER \| WebPortal \| PasswordResetURL | URL zum Kennwortrücksetzungsportal. Diese Adresse wird zur Navigation genutzt. |
| Common \| MailNotification \| DefaultCulture | Der Konfigurationsparameter enthält die Standardsprachkultur, in der E-Mail Benachrichtigungen versendet werden, wenn für einen Empfänger keine Sprachkultur ermittelt werden kann. |
| Common \| MailNotification \| Signature | Angaben zur Signatur in automatisch aus Mailvorlagen generierten E-Mails. |
| Common \| MailNotification \| Signature \| Caption | Unterschrift unter die Grußformel. |
| Common \| MailNotification \| Signature \| Company | Name des Unternehmens. |
| Common \| MailNotification \| Signature \| Link | Link zur Firmen Webseite. |
| Common \| MailNotification \| SMTPAccount | Name des Benutzerkontos zur Authentifizierung am SMTP Server. |
| Common \| MailNotification \| SMTPDomain | Domäne des Benutzerkontos zur Authentifizierung am SMTP Server. |
| Common \| MailNotification \| SMTPPassword | Kennwort des Benutzerkontos zur Authentifizierung am SMTP Server. |
| Common \| MailNotification \| SMTPPort | Port des SMTP-Dienstes auf dem SMTP Server (Standard: 25). |

| Konfigurationsparameter | Beschreibung |
| --- | --- |
| Common \| MailNotification \| SMTPRelay | SMTP Server zum Versenden von Benachrichtigungen. |
| Common \| MailNotification \| SMTPUseDefaultCredentials | Ist der Konfigurationsparameter aktiviert, werden zur Authentifizierung am SMTP Server die Credentials des One Identity Manager Services verwendet. Ist der Konfigurationsparameter nicht aktiviert werden die in den Konfigurationsparametern **Common \| MailNotification \| SMTPDomain** und **Common \| MailNotification \| SMTPAccount** beziehungsweise **Common \| MailNotification \| SMTPPassword** hinterlegten Anmeldeinformationen verwendet werden. |
| Common \| ProcessState \| PropertyLog | Bei Aktivierung des Konfigurationsparameters werden Änderungen einzelner Werte aufgezeichnet und in der Prozessansicht angezeigt. |

# 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 besuchen Sie https://www.oneidentity.com/company/contact-us.aspx oder rufen Sie + 1-800-306-9329 an.

## 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

## A

## B



## C

## D



## E

## F



## G



## M



## P



## R



## S

## U



## W



## Z