One Identity Manager 9.2

Administrationshandbuch für das SAP R/3 Compliance Add-on

Legende

WARNUNG: Das Symbol WARNUNG weist auf ein potenzielles Risiko von Körperverletzungen oder Sachschäden hin, für das Sicherheitsvorkehrungen nach Industriestandard empfohlen werden. Dieses Symbol ist oft verbunden mit elektrischen Gefahren bezüglich Hardware.

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

One Identity Manager Administrationshandbuch für das SAP R/3 Compliance Add-on
Aktualisiert - 29. September 2023, 05:04 Uhr

Die aktuellsten Versionen der Produktdokumentation finden Sie unter One Identity Manager Dokumentation.

Inhalt

SAP Funktionen und Identity Audit ... **5**
One Identity Manager Benutzer für die Verwaltung von SAP Funktionen ... 6
Voraussetzungen für die Einrichtung von SAP Funktionen ... 8
Konfigurationsparameter für SAP Funktionen ... 9

Erstellen eines Synchronisationsprojekts für die Synchronisation von SAP Berechtigungsobjekten ... **10**
Synchronisation von Berechtigungen mit sich überschneidenden Ausprägungen ... 11

Einrichten von SAP Funktionen ... **13**
Funktionsdefinitionen erstellen ... 14
Allgemeine Stammdaten einer Funktionsdefinition ... 15
Berechtigungsdefinitionen im Berechtigungseditor erstellen ... 17
Hinweise für die Berechtigungsdefinition ... 18
Eigenschaften von Berechtigungsdefinitionen und ihren Werten ... 18
Verwenden von Variablen ... 21
Vollständigkeit der Berechtigungsobjekte prüfen ... 23
Arbeitskopien aktivieren ... 23
Ermitteln unzulässiger Berechtigungen ... 24
Beispiele für SAP Funktionen ... 30
Funktionsdefinitionen bearbeiten ... 35
Überblick über Funktionsdefinitionen ... 36
Berechtigungsübersicht ... 36
Arbeitskopien erstellen ... 37
Funktionsdefinitionen exportieren ... 37
Arbeitskopien exportieren ... 38
Funktionsausprägungen definieren ... 40
Stammdaten von Funktionsausprägungen ... 41
Definition der Feldvariablen prüfen ... 42
Überblick über die Funktionsausprägung ... 42
Variablensets für Berechtigungsdefinitionen erstellen und bearbeiten ... 43
Stammdaten eines Variablensets ... 43
In SAP Funktionen verwendete Variablen übernehmen ... 45

Variablensets kopieren ... 45
Überblick über ein Variablenset ... 46
Risikomindernde Maßnahmen an SAP Funktionen zuweisen ... 46
Risikomindernde Maßnahmen an Funktionsdefinitionen zuweisen ... 47
Risikomindernde Maßnahmen für SAP Funktionen erstellen ... 47
Basisdaten für SAP Funktionen ... 48
SAP Funktionskategorien ... 48
Unternehmensbereiche ... 49
Pflege von SAP Funktionen ... 51
Alle Funktionsdefinitionen exportieren ... 52
Funktionsdefinitionen importieren ... 53

Complianceregeln für SAP Funktionen ... 56
Regelbedingungen für SAP Funktionen ... 56
Risikomindernde Maßnahmen für Complianceregeln mit SAP Funktionen ... 58
Weitere Berichte über Regelverletzungen ... 58

Risikomindernde Maßnahmen für SAP Funktionen ... 60
Stammdaten für risikomindernde Maßnahmen erfassen ... 61
Überblick über eine risikomindernde Maßnahme ... 61
Funktionsdefinitionen an risikomindernde Maßnahmen zuweisen ... 62
Risikominderung für SAP Funktionen berechnen ... 63

Anhang: Konfigurationsparameter für SAP Funktionen ... 64

Anhang: Standardprojektvorlage für das Modul SAP R/3 Compliance Add-on ... 66

Anhang: Referenzierte SAP R/3-Tabellen und BAPI-Aufrufe ... 68

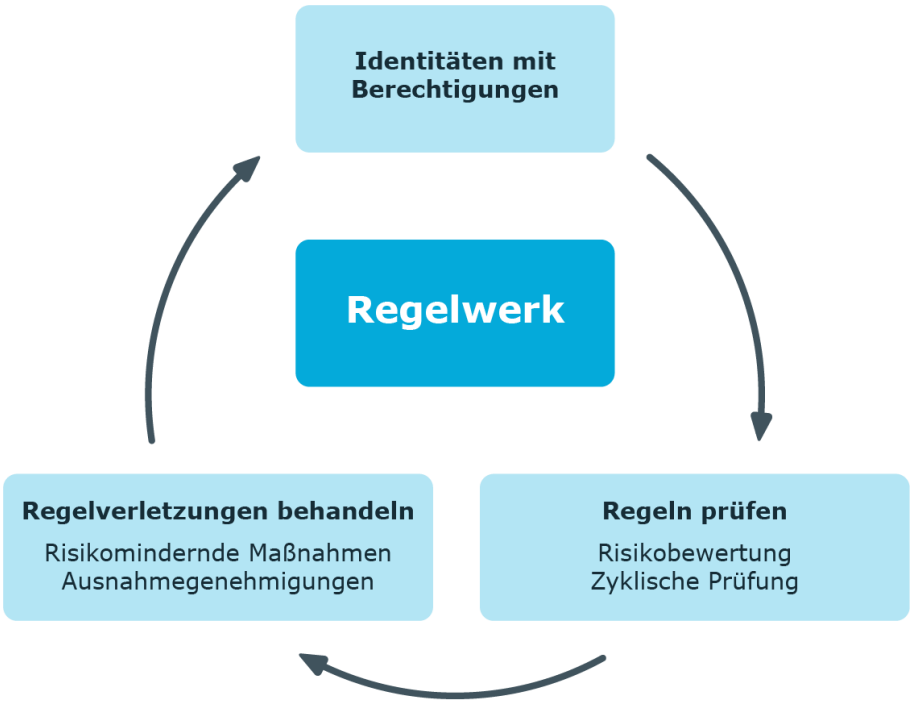
Über uns ... 69
Kontaktieren Sie uns ... 69
Technische Supportressourcen ... 69

Index ... 70

SAP Funktionen und Identity Audit

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

Abbildung 1: Identity Audit im One Identity Manager



Neben den Möglichkeiten der Regelprüfung, bietet der One Identity Manager für SAP R/3-Zielsysteme eine sehr detaillierte Überprüfung effektiver Berechtigungen der SAP Benutzerkonten an. Durch die Verbindung der SAP Benutzerkonten zu Identitäten können auch Kombinationen von SAP Berechtigungen überprüft werden, die eine Identität über verschiedene SAP Benutzerkonten erhält. Potentiell gefährliche Berechtigungen und

Berechtigungskombinationen können auf diese Weise leicht erkannt und geeignete Maßnahmen ergriffen werden.

SAP Berechtigungen werden auf der Basis der für ein Benutzerkonto zulässigen SAP Applikationen und Berechtigungsobjekte überprüft. Dafür definieren Sie im One Identity Manager SAP Funktionen, welche die zu prüfenden SAP Applikationen und Berechtigungsobjekte zusammenfassen. Der One Identity Manager ermittelt alle SAP Rollen und Profile, denen genau diese Berechtigungsobjekte zugeordnet sind. Benutzerkonten treffen die SAP Funktionen, wenn sie Mitglied in den ermittelten SAP Rollen und Profilen sind.

Um zu überprüfen, ob im Unternehmen potentiell gefährliche SAP Berechtigungen vergeben sind, definieren Sie SAP Funktionen für diese kritischen Berechtigungen. Über Complianceregeln ermitteln Sie, welche Identitäten diese SAP Funktionen treffen.

Erhalten Identitäten die SAP Berechtigungen über Bestellungen im IT Shop, können mit den entsprechenden Genehmigungsverfahren unzulässige Berechtigungen bereits bei der Bestellung erkannt und entsprechend weiter behandelt werden. Ausführliche Informationen zu Genehmigungsverfahren im IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Auf Basis dieser Informationen können Sie Korrekturen an den Daten im One Identity Manager vornehmen und in die angebundene SAP R/3-Umgebung übertragen. Durch die im One Identity Manager integrierte Reportfunktion können die Informationen für entsprechende Prüfungen bereitgestellt werden.

HINWEIS: Um SAP Funktionen einrichten und auswerten zu können, müssen das Modul SAP R/3 Compliance Add-on und das Modul Complianceregeln vorhanden sein.

HINWEIS: Die Berechtigungen in den Tochtersystemen einer Zentralen Benutzerverwaltung können nicht durch SAP Funktionen überprüft werden.

One Identity Manager Benutzer für die Verwaltung von SAP Funktionen

In die Verwaltung von SAP Funktionen sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Administratoren für Complianceregeln	Die Administratoren müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Erstellen die Basisdaten für die Erstellung des Regelwerks. • Erstellen die Complianceregeln und weisen die

Benutzer	Aufgaben
	Regelverantwortlichen zu. • Können bei Bedarf die Regelprüfung starten und Regelverletzungen einsehen. • Erstellen Berichte über Regelverletzungen. • Definieren SAP Funktionen und ordnen diesen Verantwortliche zu. • Definieren die Funktionsausprägungen und Variablensets für SAP Funktionen. • Erfassen risikomindernde Maßnahmen. • Erstellen und bearbeiten Risikoindex-Berechnungsvorschriften. • Überwachen die Identity Audit Funktionen. • Administrieren die Anwendungsrollen für Regelverantwortliche, Ausnahmegenehmiger und Attestierer. • Richten bei Bedarf weitere Anwendungsrollen ein.
Verantwortliche für die Pflege der SAP Funktionen	Die Administratoren müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Pflege SAP Funktionen** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind inhaltlich für die SAP Funktionen verantwortlich. • Bearbeiten die Arbeitskopien der Funktionsdefinitionen, für die sie verantwortlich sind. • Definieren die Funktionsausprägungen und Variablensets für SAP Funktionen. • Weisen risikomindernde Maßnahmen zu.
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte

Benutzer	Aufgaben
	Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne.
Compliance & Security Officer	Compliance & Security Officer müssen der Anwendungsrolle **Identity & Access Governance | Compliance & Security Officer** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sehen im Web Portal alle Compliance-relevanten Informationen und deren Auswertungen. Dazu gehören Attestierungsrichtlinien, Unternehmensrichtlinien und Richtlinienverletzungen, Complianceregeln und Regelverletzungen, kritische SAP Funktionen sowie Risikoindex-Berechnungsvorschriften. • Können Attestierungsrichtlinien bearbeiten.

Voraussetzungen für die Einrichtung von SAP Funktionen

Damit der One Identity Manager die effektiven SAP Berechtigungen anhand der SAP Funktionen prüfen kann, müssen alle Informationen zu SAP Berechtigungen, SAP Benutzerkonten, SAP Rollen und SAP Profilen in die One Identity Manager-Datenbank übertragen werden.

Um SAP Funktionen einzurichten

1. Aktivieren Sie im Designer die Konfigurationsparameter **QER \| ComplianceCheck** und **TargetSystem \| SAPR3 \| SAPRights**.

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

2. Erstellen Sie ein Synchronisationsprojekt für die Synchronisation der benötigten SAP Schematypen und starten Sie die Synchronisation.

Detaillierte Informationen zum Thema

- Erstellen eines Synchronisationsprojekts für die Synchronisation von SAP Berechtigungsobjekten auf Seite 10

Konfigurationsparameter für SAP Funktionen

Über Konfigurationsparameter konfigurieren Sie die Grundeinstellungen zum Systemverhalten. Der One Identity Manager stellt für verschiedene Konfigurationsparameter Standardeinstellungen zur Verfügung. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.

Die Konfigurationsparameter sind in den One Identity Manager Modulen definiert. Jedes One Identity Manager Modul kann zusätzliche Konfigurationsparameter installieren. Einen Überblick über alle Konfigurationsparameter finden Sie im Designer in der Kategorie **Basisdaten > Allgemein > Konfigurationsparameter**.

Weitere Informationen finden Sie unter Konfigurationsparameter für SAP Funktionen auf Seite 64.

2

Erstellen eines Synchronisationsprojekts für die Synchronisation von SAP Berechtigungsobjekten

SAP Berechtigungen werden auf der Basis der für ein SAP Benutzerkonto zulässigen SAP Applikationen und Berechtigungsobjekte überprüft. Um SAP Funktionen erstellen zu können, müssen die Berechtigungsobjekte und SAP Applikationen in die One Identity Manager-Datenbank eingelesen werden. Erstellen Sie für jeden Mandanten ein Synchronisationsprojekt, über das die benötigten Schematypen synchronisiert werden können. Dafür wird eine separate Projektvorlage bereitgestellt.

Verwenden Sie den Synchronization Editor, um die Synchronisation zwischen One Identity Manager-Datenbank und SAP R/3-Umgebung einzurichten.

HINWEIS: Pro Zielsystem und genutzter Standardprojektvorlage kann genau ein Synchronisationsprojekt erstellt werden.

Um ein Synchronisationsprojekt für SAP Berechtigungsobjekte einzurichten

1. Erstellen Sie ein initiales Synchronisationsprojekt wie im Handbuch One Identity Manager Administrationshandbuch für die Anbindung einer SAP R/3-Umgebung beschrieben. Es gelten folgende Besonderheiten:

   HINWEIS: Die Berechtigungen in den Tochtersystemen einer Zentralen Benutzerverwaltung können nicht durch SAP Funktionen überprüft werden. Erstellen Sie das Synchronisationsprojekt nur für einen Mandanten, der kein ZBV-System ist.

   a. Wählen Sie im Projektassistenten auf der Seite **Projektvorlage auswählen** die Projektvorlage **SAP R/3 Berechtigungsobjekte**.

   b. Die Seite **Zielsystemzugriff einschränken** wird nicht angezeigt. Das Zielsystem soll nur eingelesen werden.

   Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer SAP R/3-Umgebung*.

2. Konfigurieren und aktivieren Sie einen Zeitplan, um regelmäßige Synchronisationen auszuführen.

Ausführliche Informationen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Standardprojektvorlage für das Modul SAP R/3 Compliance Add-on auf Seite 66
- Referenzierte SAP R/3-Tabellen und BAPI-Aufrufe auf Seite 68
- Synchronisation von Berechtigungen mit sich überschneidenden Ausprägungen auf Seite 11

Synchronisation von Berechtigungen mit sich überschneidenden Ausprägungen

Wenn in der SAP R/3-Umgebung einem SAP Profil dieselbe Berechtigung mehrfach mit sich überschneidenden Wertebereichen zugewiesen ist, wird durch die Synchronisation nur eine Berechtigungszuweisung eingelesen. In die Berechtigungsprüfung gehen dann nicht alle Ausprägungen ein, die Benutzerkonten mit diesem Profil tatsächlich nutzen können.

Wahrscheinliche Ursache

Bei der Synchronisation des Schematyps `ProfileHasAuthObjectField` wird gleich die vollständige Objektliste geladen. Dabei wird pro Zuweisung einer Berechtigung an ein SAP Profil immer nur ein Datensatz selektiert. Weitere Datensätze werden ignoriert.

Lösung

Wenn für ein Profil mehrere Berechtigungszuweisungen mit sich überschneidenden Wertebereichen existieren, sollen durch die Synchronisation die niedrigste untere und die höchste obere Ausprägung eingelesen werden. Dafür müssen die Datensätze bei der Synchronisation einzeln ausgewertet werden. Die Objekte müssen per Einzelsatzzugriff eingelesen werden.

Um den Einzelsatzzugriff zu ermöglichen

1. Bearbeiten Sie im Synchronization Editor die Eigenschaften des Synchronisationsschritts **profileHasAuthObjectField**.
2. Wählen Sie den Tabreiter **Erweitert**.
3. Wählen Sie die Eigenschaft **Nachladeschwellwert** und deaktivieren Sie **Verwende Einstellungen der Startkonfiguration**.
4. Erfassen Sie einen Wert zwischen **4** und **7**.
5. Speichern Sie die Änderungen.

HINWEIS: Die Änderung des Nachladeschwellwerts kann die Synchronisationsperformance für diesen Synchronisationsschritt beeinträchtigen.

Ausführliche Informationen zur Konfiguration des Nachladeschwellwerts finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Erstellen eines Synchronisationsprojekts für die Synchronisation von SAP Berechtigungsobjekten auf Seite 10

Einrichten von SAP Funktionen

Für SAP Funktionen erstellen Sie Funktionsdefinitionen, Funktionsausprägungen und Variablensets. Eine Funktionsdefinition enthält neben allgemeinen Stammdaten die Berechtigungsdefinition. Eine Berechtigungsdefinition enthält mindestens eine SAP Applikation. Zu jeder SAP Applikation gehört mindestens ein Berechtigungsobjekt. Jedes Berechtigungsobjekt besteht aus mindestens einem Funktionselement (Aktivität oder Berechtigungsfeld) mit konkreten Ausprägungen. Ausprägungen werden als Einzelwerte oder untere und obere Bereichsgrenze angegeben. Funktionselemente können je Berechtigungsobjekt mehrfach aufgelistet werden.

Eine SAP Funktion kann für verschiedene Ausprägungen genutzt werden. Dafür setzen Sie in der Berechtigungsdefinition Variablen ein. Die konkreten Werte der Variablen werden in Variablensets zusammengestellt und in den Funktionsausprägungen angewendet.

Abbildung 2: Struktur einer Berechtigungsdefinition

```
Funktionsdefinition
   SAP Applikation (Applikationstyp)
      Berechtigungsobjektklasse
         Berechtigungsobjekt
            Funktionselement mit Einzelwert oder Wertebereich
            ...
         ...
      ...
   ...
```

Um eine SAP Funktion einzurichten

1. Erstellen Sie eine Funktionsdefinition.
   - (Optional) Weisen Sie bei Bedarf Verantwortliche, eine Funktionskategorie oder einen Unternehmensbereich zu.
2. Erstellen Sie die Berechtigungsdefinition.
   - Berücksichtigen Sie die Erläuterungen zur Ermittlung unzulässiger Berechtigungen.
   - Beachten Sie die Hinweise für die Berechtigungsdefinition.
   - Nutzen Sie für die Werte oder Bereichsgrenzen bei Bedarf Variablen.

3. Prüfen Sie die Berechtigungsobjekte auf Vollständigkeit.
4. (Optional) Weisen Sie der Funktionsdefinition risikomindernde Maßnahmen zu, die umgesetzt werden sollen, wenn durch die SAP Funktion unzulässige Berechtigungen ermittelt werden.
5. Um die Funktionsdefinition für die Berechtigungsprüfung nutzen zu können, aktivieren Sie die Arbeitskopie dieser Funktionsdefinition.
6. Erstellen Sie mindestens eine Funktionsausprägung für diese Funktionsdefinition.

Um alle Identitäten zu ermitteln, die über ihre SAP Benutzerkonten diese SAP Funktion treffen, verwenden Sie die SAP Funktion in Complianceregeln.

Detaillierte Informationen zum Thema

- Funktionsdefinitionen erstellen auf Seite 14
- Basisdaten für SAP Funktionen auf Seite 48
- Berechtigungsdefinitionen im Berechtigungseditor erstellen auf Seite 17
- Ermitteln unzulässiger Berechtigungen auf Seite 24
- Hinweise für die Berechtigungsdefinition auf Seite 18
- Verwenden von Variablen auf Seite 21
- Vollständigkeit der Berechtigungsobjekte prüfen auf Seite 23
- Risikomindernde Maßnahmen an SAP Funktionen zuweisen auf Seite 46
- Arbeitskopien aktivieren auf Seite 23
- Funktionsausprägungen definieren auf Seite 40
- Complianceregeln für SAP Funktionen auf Seite 56

Funktionsdefinitionen erstellen

Für jede neue Funktionsdefinition wird in der Datenbank eine Arbeitskopie angelegt. Erst mit Aktivierung der Arbeitskopie werden die Änderungen auf die produktive Funktionsdefinition übertragen. SAP Berechtigungen werden nur anhand aktivierter Funktionsdefinitionen überprüft.

Um eine neue Funktionsdefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Funktionsdefinitionen**.
2. Klicken Sie in der Ergebnisliste .
3. Erfassen Sie die Stammdaten der Funktionsdefinition.
4. Speichern Sie die Änderungen.

   Es wird eine Arbeitskopie angelegt.

5. Wählen Sie die Aufgabe **Berechtigungseditor** und erstellen Sie die Berechtigungsdefinition.
6. Wählen Sie die Aufgabe **Arbeitskopie aktivieren** und bestätigen Sie die Sicherheitsabfrage mit **OK**.

   Es wird eine aktive Funktionsdefinition in der Datenbank angelegt. Die Arbeitskopie bleibt bestehen und wird für nachfolgende Änderungen genutzt.

Verwandte Themen

- Allgemeine Stammdaten einer Funktionsdefinition auf Seite 15
- Berechtigungsdefinitionen im Berechtigungseditor erstellen auf Seite 17
- Arbeitskopien aktivieren auf Seite 23

Allgemeine Stammdaten einer Funktionsdefinition

Für eine Funktionsdefinition erfassen Sie folgende Stammdaten.

Tabelle 2: Stammdaten einer Funktionsdefinition

Eigenschaft	Beschreibung
Funktionsdefinition	Bezeichnung der SAP Funktion.
Unternehmensbereich	Unternehmensbereich, für den die SAP Funktion gültig ist.
Funktionskategorie	Gruppierungskriterium für die SAP Funktion. Um eine neue Funktionskategorie zu erstellen, klicken Sie . Erfassen Sie den Namen und eine Beschreibung der Funktionskategorie.
Verantwortliche	Anwendungsrolle, deren Mitglieder inhaltlich für diese Funktionsdefinition verantwortlich sind. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Berechtigungsobjekte	Freitextfeld zum Erfassen von Informationen über die Berechtigungsobjekte, die in der Funktionsdefinition genutzt werden.
Risikoindex	Gibt das Risiko für das Unternehmen an, wenn ein SAP Benutzerkonto diese SAP Funktion trifft. Stellen Sie über den Schieberegler einen Wert zwischen **0** und **1** ein. **0**: kein Risiko **1**: Jedes SAP Benutzerkonto, das die SAP Funktion trifft, ist ein Problem.

Eigenschaft	Beschreibung
	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 SAP Funktion wird um die Signifikanzminderung aller zugewiesenen risikomindernden Maßnahmen reduziert. Der Risikoindex (reduziert) wird für die originale SAP Funktion berechnet. Um diesen Wert in die Arbeitskopie zu übernehmen, führen Sie die Aufgabe **Arbeitskopie erstellen** aus. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Der Wert wird durch den One Identity Manager berechnet und kann nicht bearbeitet werden.
Schweregrad	Gibt an, welche Bedeutung es für das Unternehmen oder den zugeordneten Unternehmensbereich hat, wenn SAP Benutzerkonten diese SAP Funktion treffen. Erfassen Sie einen Wert zwischen **0** und **1**. **0**: nur zur Information **1**: Jedes SAP Benutzerkonto, das die SAP Funktion trifft, erfordert Änderungen an den betroffenen SAP Berechtigungen.
Auswirkung	Gibt in verbaler Beschreibung an, welche Auswirkungen es für das Unternehmen oder den zugeordneten Unternehmensbereich hat, wenn SAP Benutzerkonten diese SAP Funktion treffen. In der Standardinstallation wird die Werteliste {**Niedrig**, **Mittel**, **Hoch**, **Kritisch**} angezeigt.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Arbeitskopie	Angabe, ob es sich um die Arbeitskopie der Funktionsdefinition handelt.

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

Detaillierte Informationen zum Thema

- SAP Funktionskategorien auf Seite 48
- Pflege von SAP Funktionen auf Seite 51
- Risikomindernde Maßnahmen für SAP Funktionen auf Seite 60

Berechtigungsdefinitionen im Berechtigungseditor erstellen

Über den Berechtigungseditor erstellen Sie die Berechtigungsdefinition der SAP Funktion. Dafür stellen Sie die SAP Applikationen und Berechtigungsobjekte zusammen, die durch die SAP Funktion abgedeckt werden sollen.

Um die Berechtigungsdefinition zusammenzustellen

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Arbeitskopien von Funktionsdefinitionen**.
2. Wählen Sie in der Ergebnisliste die Funktionsdefinition.
3. Wählen Sie die Aufgabe **Berechtigungseditor**.
4. Wählen Sie eine der folgenden Aufgaben.
    - **1. Hinzufügen durch Menüvorlage**

      Wählen Sie, aus welchem Menü Sie die Menüeinträge auswählen möchten und das SAP System, dessen Menübaum angezeigt werden soll. Wählen Sie anschließend aus dem Menübaum einen Menüeintrag aus. Als zusätzliche Information werden im Menübaum die mit einem Menüeintrag verknüpften Transaktionscodes in Klammern angezeigt.

      Es werden alle Transaktionen und deren zugeordnete Berechtigungsobjekte geladen, die über den ausgewählten Menüeintrag oder seine untergeordneten Menüeinträge aufgerufen werden können.
    - **2. Hinzufügen durch SAP Applikation**

      Wählen Sie den Typ der SAP Applikation und die SAP Applikation, deren Berechtigungsobjekte in den Berechtigungseditor geladen werden sollen. Es werden alle Berechtigungsobjekte eingefügt, die mit der ausgewählten SAP Applikation verknüpft sind. Sie können einen Filter definieren, um die Liste der zur Verfügung stehenden SAP Applikationen einzuschränken.
    - **3. Hinzufügen durch vorhandene Funktionsdefinition**

      Wählen Sie eine vorhandene Funktionsdefinition aus, deren Berechtigungsdefinition in den Berechtigungseditor geladen werden soll.

      Es werden nur die aktivierten Funktionsdefinitionen zur Auswahl angeboten.
5. Legen Sie die Details für die einzelnen Funktionselemente im Berechtigungseditor fest.
6. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Eigenschaften von Berechtigungsdefinitionen und ihren Werten auf Seite 18
- Hinweise für die Berechtigungsdefinition auf Seite 18
- Verwenden von Variablen auf Seite 21

Hinweise für die Berechtigungsdefinition

Beim Erstellen einer Berechtigungsdefinition im Berechtigungseditor berücksichtigen Sie folgende Hinweise:

- Um zu einem Berechtigungsobjekt einen zusätzlichen Wert für eine Aktivität hinzuzufügen, klicken Sie **+**. Mehrere zulässige Werte von Aktivitäten können auch als ODER- oder UND-Verknüpfungen erfasst werden.
- Um zu einem Berechtigungsobjekt einen zusätzlichen Wert für ein Berechtigungsfeld hinzuzufügen, klicken Sie **C** neben diesem Berechtigungsfeld.
- Das selbe Berechtigungsobjekt kann innerhalb einer Berechtigungsdefinition nicht mehrfach eingefügt werden.
- ODER- und UND-Verknüpfungen können für Aktivitäten unterhalb eines Berechtigungsobjekts nicht kombiniert werden. Wenn eine Aktivität eine UND-Verknüpfung enthält, dürfen unterhalb des selben Berechtigungsobjekts keine weiteren Aktivitäten definiert sein.
- ODER- und UND-Verknüpfungen können für das selbe Berechtigungsfeld unterhalb eines Berechtigungsobjekts nicht kombiniert werden. Wenn ein Berechtigungsfeld eine UND-Verknüpfung enthält, darf unterhalb des selben Berechtigungsobjekts dieses Berechtigungsfeld nicht erneut definiert sein.

Detaillierte Informationen zum Thema

- Berechtigungsdefinitionen im Berechtigungseditor erstellen auf Seite 17
- Ermitteln unzulässiger Berechtigungen auf Seite 24

Verwandte Themen

- Beispiele für SAP Funktionen auf Seite 30
- Regelbedingungen für SAP Funktionen auf Seite 56

Eigenschaften von Berechtigungsdefinitionen und ihren Werten

Die Funktionsweise des Berechtigungseditors ist an den Berechtigungseditor der SAP GUI angelehnt. Die einzelnen Spalten im Berechtigungseditor haben folgende Bedeutung.

Tabelle 3: Eigenschaften einer Berechtigungsdefinition

Eigenschaft	Beschreibung
Funktionsdefinition / SAP Applikation / Berechtigung /	Hierarchie der Funktionsdefinition. Es werden die SAP Applikationen, ihre zugehörigen Berechtigungsobjekte und Funktionselemente in einer Baumstruktur abgebildet.

Eigenschaft	Beschreibung
Funktionselement	
Bearbeitungsstatus	Bearbeitungsstatus der Objekte der Baumstruktur. 🟠: Für das Funktionselement ist kein Wert festgelegt. 🟢: Für das Funktionselement ist ein Wert festgelegt.
Hinzufügen	Klicken Sie **+**, um weitere Objekte der Berechtigungsdefinition hinzuzufügen. Es wird ein untergeordnetes Objekt hinzugefügt. Klicken Sie **C**, um das Funktionselement zu duplizieren.
Entfernen	Klicken Sie **-**, um Objekte aus der Berechtigungsdefinition zu entfernen.
Beschreibung	Beschreibung des Objekts.
Beliebig	Klicken Sie *, um den Wert eines Funktionselements auf * (beliebiger Wert) festzulegen.
Wert / Untere Bereichsgrenze	Zulässige Werte für das Funktionselement. Beispielsweise können Sie die SAP Berechtigungen auf konkrete SAP Gruppen einschränken. Wenn Sie einen Wertebereich festlegen, geben Sie hier den unteren Grenzwert an. Werte können als Variablen eingefügt werden. Es können auch Systemvariablen genutzt werden. In den Werten können Platzhalter genutzt werden. Weitere Informationen finden Sie unter Syntaxbeispiele für Werte auf Seite 19.
Obere Bereichsgrenze	Oberer Grenzwert für den Wertebereich eines Funktionselements. Werte können als Variablen eingefügt werden. Mit **,** oder **+** verknüpfte Werte und * sind nicht zulässig. Wenn **Wert / Untere Bereichsgrenze** mit **+** oder **,** verknüpfte Werte oder * enthält, kann keine obere Bereichsgrenze erfasst werden.

Tabelle 4: Syntaxbeispiele für Werte

Syntax (Beispiel)	SAP Berechtigung wird geprüft auf	Beispiele für Feldwerte
*	beliebige Werte Kann nur als Einzelwert genutzt werden. Es kann keine obere Bereichsgrenze angegeben werden.	ab oder 1234
beliebige Zeichenkette	exakt den angegebenen Wert	ab

Syntax (Beispiel)	SAP Berechtigung wird geprüft auf	Beispiele für Feldwerte
(ab)		
[*]	den Wert *	*
Zeichenkette[*] (ab[*])	Werte, die exakt diese Zeichenkette und * enthalten	ab*
Zeichenkette* (ab*)	Werte, die mit der angegebenen Zeichenkette beginnen und mit einer beliebigen Zeichenkette enden Kann nur als Einzelwert genutzt werden. Es kann keine obere Bereichsgrenze angegeben werden.	abcd oder ab*
ODER-Verknüpfung (01,02,78)	einen der in der Liste enthaltenen Werte ODER-Verknüpfungen können nicht für die obere Bereichsgrenze genutzt werden. Kann nur als Einzelwert genutzt werden. Es kann keine obere Bereichsgrenze angegeben werden.	01 oder 02 oder 78
UND-Verknüpfung (01+02+78)	alle in der Liste enthaltenen Werte UND-Verknüpfungen können nicht für die obere Bereichsgrenze genutzt werden. Kann nur als Einzelwert genutzt werden. Es kann keine obere Bereichsgrenze angegeben werden.	01 und 02 und 78
[*],[,],[+] (FM[+]7)	Werte, die das Sonderzeichen enthalten	FM+7
Variable (Var)	die in der Variable hinterlegten Werte	
Systemvariable ($Var)	die in der Systemvariable hinterlegten Werte	

Innerhalb einer SAP Applikation müssen alle Funktionselemente erfüllt sein, die in einer separaten Zeile definiert sind, damit die SAP Funktion getroffen wird. Soll die SAP Funktion nur getroffen werden, wenn ein SAP Profil eine von mehreren möglichen Ausprägungen eines Funktionselements besitzt, definieren Sie diese Ausprägungen als ODER-Verknüpfung. Soll die SAP Funktion getroffen werden, wenn ein SAP Profil alle Ausprägungen eines Funktionselements besitzt, definieren Sie diese Ausprägungen als UND-Verknüpfung.

Um die Eigenschaften des ausgewählten Objekts zu bearbeiten

- Doppelklicken Sie im Berechtigungseditor auf ein Funktionselement.

  Sie können die Beschreibung des Funktionselements sowie die untere und obere Bereichsgrenze ändern.

Tabelle 5: Eigenschaften eines Funktionselements

Eigenschaft	Beschreibung
Typ	Angabe, ob es sich bei dem ausgewählten Funktionselement um eine Aktivität oder ein Berechtigungsfeld handelt.
Bezeichnung	Bezeichnung des Funktionselements.
Untere Bereichsgrenze, Obere Bereichsgrenze	Zulässige Werte für das Funktionselement. Wenn Sie einen Wertebereich festlegen, geben Sie den unteren und oberen Grenzwert an. Werte können als Variablen eingefügt werden. Klicken Sie, um Variablen aus den vorhandenen Variablendefinitionen auszuwählen.
Beschreibung	Detaillierte Beschreibung des Funktionselements.

Detaillierte Informationen zum Thema

- Hinweise für die Berechtigungsdefinition auf Seite 18
- Verwenden von Variablen auf Seite 21
- Variablensets für Berechtigungsdefinitionen erstellen und bearbeiten auf Seite 43
- Berechtigungsdefinitionen im Berechtigungseditor erstellen auf Seite 17

Verwenden von Variablen

Für Funktionselemente können in der Berechtigungsdefinition konkrete Werte angegeben werden. Um die Funktionsdefinition für verschiedene Funktionsausprägungen zu nutzen, können Sie stattdessen Variablen einsetzen. Dafür gelten folgende Festlegungen.

- Variablenname
  - beginnt mit einem Buchstaben
  - enthält nur Buchstaben, Zahlen und den Unterstrich
  - ist von $-Zeichen eingeschlossen

  Beispiel: Var_01

  HINWEIS: Variablennamen dürfen nicht mit dem Namen von Systemvariablen beginnen.
- Wert

Syntax (Beispiel)	SAP Berechtigung wird geprüft auf	Beispiele für Feldwerte
*	beliebige Werte	ab oder

Syntax (Beispiel)	SAP Berechtigung wird geprüft auf	Beispiele für Feldwerte
	Kann nur als Einzelwert genutzt werden. Es kann keine obere Bereichsgrenze angegeben werden.	1234
beliebige Zeichenkette (ab)	exakt den angegebenen Wert	ab
[*]	den Wert *	*
Zeichenkette[*] (ab[*])	Werte, die exakt diese Zeichenkette und * enthalten	ab*
Zeichenkette* (ab*)	Werte, die mit der angegebenen Zeichenkette beginnen und mit einer beliebigen Zeichenkette enden Kann nur als Einzelwert genutzt werden. Es kann keine obere Bereichsgrenze angegeben werden.	abcd oder ab*
ODER-Verknüpfung (01,02,78)	einen der in der Liste enthaltenen Werte ODER-Verknüpfungen können nicht für die obere Bereichsgrenze genutzt werden. Kann nur als Einzelwert genutzt werden. Es kann keine obere Bereichsgrenze angegeben werden.	01 oder 02 oder 78
UND-Verknüpfung (01+02+78)	alle in der Liste enthaltenen Werte UND-Verknüpfungen können nicht für die obere Bereichsgrenze genutzt werden. Kann nur als Einzelwert genutzt werden. Es kann keine obere Bereichsgrenze angegeben werden.	01 und 02 und 78
[*],[,],[+] (FM[+]7)	Werte, die das Sonderzeichen enthalten	FM+7

Neben den selbstdefinierten Variablen können in der Berechtigungsdefinition auch Systemvariablen verwendet werden. Systemvariablen haben folgende Syntax: `${character}+` (Beispiel: $AUFART).

Variablen müssen bei der Berechtigungsprüfung eindeutig identifizierbar sein. Daher dürfen die Variablennamen selbstdefinierter Variablen nicht den Systemvariablen entsprechen oder mit dem Namen von Systemvariablen beginnen.

Verwandte Themen

- Berechtigungsdefinitionen im Berechtigungseditor erstellen auf Seite 17
- Stammdaten eines Variablensets auf Seite 43

Vollständigkeit der Berechtigungsobjekte prüfen

Über diese Aufgabe prüft der One Identity Manager, ob alle Berechtigungsobjekte, die zu einer SAP Applikation gehören, in der Berechtigungsdefinition vorkommen.

Um eine Berechtigungsdefinition auf Vollständigkeit zu prüfen

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Arbeitskopien von Funktionsdefinitionen**.
2. Wählen Sie in der Ergebnisliste die Funktionsdefinition.
3. Wählen Sie die Aufgabe **Berechtigungseditor**.
4. Wählen Sie die Aufgabe **Vollständigkeit der Berechtigungsobjekte prüfen**.

   Fehlende Berechtigungsobjekte werden in einem separaten Fenster angezeigt.
5. Aktivieren Sie die Option **Aufnehmen** an den Berechtigungsobjekten, die Sie in die Berechtigungsdefinition einfügen wollen.
6. Wenn alle fehlenden Berechtigungsobjekte bearbeitet sind, klicken Sie **OK**.

   Die Berechtigungsobjekte können jetzt im Berechtigungseditor bearbeitet werden.

Verwandte Themen

- Berechtigungsdefinitionen im Berechtigungseditor erstellen auf Seite 17

Arbeitskopien aktivieren

SAP Berechtigungen werden nur anhand aktivierter SAP Funktionen überprüft. Mit der Aktivierung der Arbeitskopie werden Änderungen auf die Funktionsdefinition übertragen. Zu einer neuen Arbeitskopie wird eine aktive Funktionsdefinition angelegt.

Um Änderungen an einer Arbeitskopie in eine Funktionsdefinition zu übernehmen

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

Verwandte Themen

- Arbeitskopien erstellen auf Seite 37
- Funktionsdefinitionen erstellen auf Seite 14

Ermitteln unzulässiger Berechtigungen

SAP Berechtigungen werden auf der Basis der für ein SAP Benutzerkonto zulässigen SAP Applikationen und Berechtigungsobjekte überprüft. Um zu ermitteln, ob im Unternehmen potentiell gefährliche Berechtigungen vergeben sind, definieren Sie SAP Funktionen, welche die zu prüfenden SAP Applikationen und Berechtigungsobjekte zusammenfassen. Der One Identity Manager gleicht alle den Einzelprofilen zugeordneten Berechtigungsobjekte mit der Berechtigungsdefinition in der SAP Funktion ab. Er ermittelt auf diesem Weg alle SAP Rollen und Profile, denen genau diese Berechtigungsobjekte über die Summe ihrer Einzelprofile zugeordnet sind.

Bei der Berechtigungsprüfung wird der Konfigurationsparameter **TargetSystem | SAPR3 | SAPRights | TestWithoutTCD** ausgewertet. Der Konfigurationsparameter legt fest, ob bei der Berechtigungsprüfung die SAP Applikationen ignoriert und nur die Berechtigungsobjekte berücksichtigt werden sollen.

Konfigurationsparameter TestWithoutTCD ist nicht aktiviert (Standard)

Für die Berechtigungsprüfung gelten die folgenden Regeln:

Eine SAP Rolle oder ein SAP Profil trifft eine SAP Funktion, wenn

1. es mindestens eine der SAP Applikationen enthält, die in der SAP Funktion definiert sind,

```
Funktionsdefinition
   CHIP_CATALOG_GET_LIST (RFC-Funktionsbaustein)    ODER
      ...
   SE16 (Transaktion)                               ODER
      ...
   SU01 (Transaktion)
      ...
```

2. es alle in der SAP Funktion definierten Berechtigungsobjekte dieser SAP Applikation besitzt,

```
Funktionsdefinition
   SAP Applikation (Applikationstyp)
      ...
         S_TCODE                          UND
            ...
         S_TABU_DIS                       UND
            ...
         S_TABU_NAM
            ...
```

3. es alle unterschiedlichen Funktionselemente eines Berechtigungsobjekts besitzt, die in der SAP Funktion definiert sind,

```
Funktionsdefinition
   SAP Applikation (Applikationstyp)
      ...
         Berechtigungsobjekt
            ACTVT                          UND
            TABLE
```

4. mindestens eine oder alle der Ausprägungen ein und desselben Funktionselements vorhanden sind, die in der SAP Funktion definiert sind.

```
Funktionsdefinition
   SAP Applikation (Applikationstyp)
      ...
         Berechtigungsobjekt
            TABLE = USR10                  ODER
            TABLE = USR11
         Berechtigungsobjekt
            ACTVT = 01,02,03               01 ODER 02 ODER 03
         Berechtigungsobjekt
            CLASS = 01+02+03               01 UND 02 UND 03
```

Eine SAP Rolle trifft eine SAP Funktion, wenn ein SAP Profil dieser SAP Rolle die SAP Funktion trifft.

Ein SAP Profil trifft eine SAP Funktion, wenn es mindestens eine der SAP Applikationen enthält, die in der SAP Funktion definiert sind. Dabei muss das SAP Profil alle Berechtigungsobjekte dieser SAP Applikation besitzen. Ist für ein Berechtigungsobjekt ein Funktionselement mit unterschiedlichen Ausprägungen definiert, trifft das SAP Profil die SAP Funktion, wenn es mindestens eine oder alle dieser Ausprägungen besitzt.

Konfigurationsparameter TestWithoutTCD ist aktiviert

Bei der Berechtigungsprüfung werden die SAP Applikationen nicht berücksichtigt. Für die Berechtigungsprüfung gelten folgende Regeln:

Eine SAP Rolle oder ein SAP Profil trifft eine SAP Funktion, wenn

1. es alle in der SAP Funktion definierten Berechtigungsobjekte aller SAP Applikationen besitzt,

   außer den Berechtigungsobjekten, die zur Identifikation der SAP Applikationen benötigt werden,

```
Funktionsdefinition
   SAP Applikation (Applikationstyp)
      ...
         S_CTS_ADMI                          UND
            ...
   SAP Applikation (Applikationstyp)
      ...
         S_TABU_DIS                          UND
            ...
         S_TABU_NAM
            ...
```

2. es alle unterschiedlichen Funktionselemente eines Berechtigungsobjekts besitzt, die in der SAP Funktion definiert sind,

```
Funktionsdefinition
   SAP Applikation (Applikationstyp)
      ...
         Berechtigungsobjekt
            ACTVT                            UND
            TABLE
```

3. mindestens eine oder alle der Ausprägungen ein und desselben Funktionselements vorhanden sind, die in der SAP Funktion definiert sind.

```
Funktionsdefinition
   SAP Applikation (Applikationstyp)
      ...
         Berechtigungsobjekt
            TABLE = USR10                    ODER
            TABLE = USR11
         Berechtigungsobjekt
            ACTVT = 01,02,03                 01 ODER 02 ODER 03
         Berechtigungsobjekt
            CLASS = 01+02+03                 01 UND 02 UND 03
```

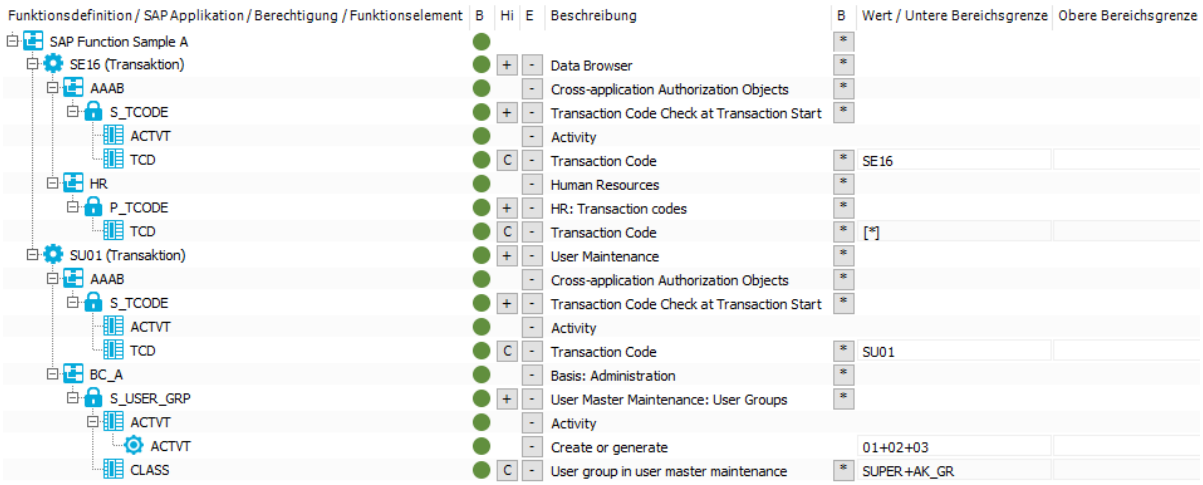
Für die Berechtigungsprüfung sind nur die Berechtigungsobjekte und ihre Ausprägungen von Interesse. Zu welchen SAP Applikationen diese Berechtigungsobjekte gehören ist nicht relevant. Das heißt, auch die Berechtigungsobjekte, die nur zur Identifikation der Applikationen genutzt werden, werden ignoriert. Folgende Berechtigungsobjekte und Funktionselemente bleiben also unberücksichtigt:

- Externer Service: S_Service mit SRV_NAME
- TADIR-Service: S_START mit AUTHOBJNAM, AUTHOBJTYP und AUTHPGMID
- RFC-Funktionsbaustein: S_RFC mit RFC_NAME
- Transaktion: S_TCODE mit TCD

Beispiele für eine Berechtigungsprüfung

Es ist eine SAP Funktion mit folgenden SAP Applikationen, Berechtigungsobjekten und Funktionselementen definiert.

Abbildung 3: Berechtigungsdefinition mit Transaktionen



Funktionsdefinition / SAP Applikation / Berechtigung / Funktionselement	B	Hi	E	Beschreibung	B	Wert / Untere Bereichsgrenze	Obere Bereichsgrenze
SAP Function Sample A					*		
SE16 (Transaktion)		+	-	Data Browser	*		
AAAB			-	Cross-application Authorization Objects	*		
S_TCODE		+	-	Transaction Code Check at Transaction Start	*		
ACTVT			-	Activity			
TCD		C	-	Transaction Code	*	SE16	
HR			-	Human Resources	*		
P_TCODE		+	-	HR: Transaction codes	*		
TCD		C	-	Transaction Code	*	[*]	
SU01 (Transaktion)		+	-	User Maintenance	*		
AAAB			-	Cross-application Authorization Objects	*		
S_TCODE		+	-	Transaction Code Check at Transaction Start	*		
ACTVT			-	Activity			
TCD		C	-	Transaction Code	*	SU01	
BC_A			-	Basis: Administration	*		
S_USER_GRP		+	-	User Master Maintenance: User Groups	*		
ACTVT			-	Activity			
ACTVT			-	Create or generate		01+02+03	
CLASS		C	-	User group in user master maintenance	*	SUPER+AK_GR	

Bei deaktiviertem Konfigurationsparameter werden durch die abgebildete SAP Funktion alle SAP Rollen und SAP Profile ermittelt, die folgende Berechtigungen besitzen:

SAP Applikation **SE16** mit
Berechtigungsobjekt **S_TCODE** mit
Funktionselement **ACTVT**
UND
Funktionselement **TCD** mit der Ausprägung **SE16**

UND

Berechtigungsobjekt **P_TCODE** mit
Funktionselement **TCD** mit genau der Ausprägung *

ODER

SAP Applikation **SU01** mit
Berechtigungsobjekt **S_TCODE** mit
Funktionselement **ACTVT**
UND
Funktionselement **TCD** mit mindestens der Ausprägung **SU01**

UND

Berechtigungsobjekt **S_USER_GRP** mit
Funktionselement **ACTVT** mit mindestens den Ausprägungen **01** UND **02** UND **03**
UND
Funktionselement **CLASS** mit mindestens der Ausprägung **SUPER** UND **AK_GR**

Bei aktiviertem Konfigurationsparameter werden durch die abgebildete SAP Funktion alle SAP Rollen und SAP Profile ermittelt, die folgende Berechtigungen besitzen:

Berechtigungsobjekt **P_TCODE** mit
Funktionselement **TCD** mit genau der Ausprägung *

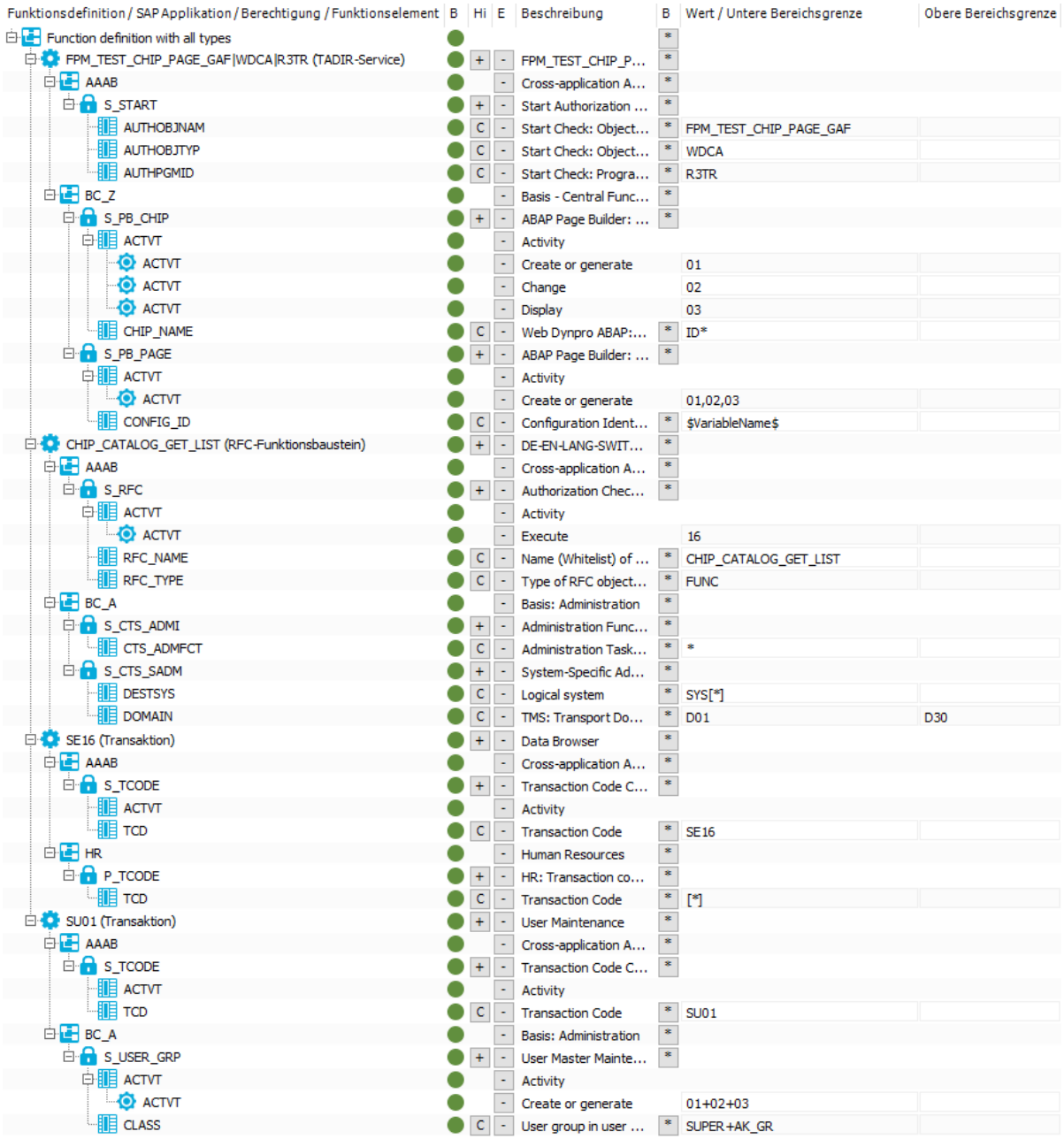
UND

Berechtigungsobjekt **S_USER_GRP** mit

Funktionselement **ACTVT** mit mindestens den Ausprägungen **01** UND **02** UND **03**
UND
Funktionselement **CLASS** mit mindestens der Ausprägung **SUPER** UND **AK_GR**

Folgende Funktionsdefinition enthält verschiedene SAP Applikationen mit unterschiedlichem Applikationstyp.

Abbildung 4: Berechtigungsdefinition mit verschiedenen Applikationstypen



Funktionsdefinition / SAP Applikation / Berechtigung / Funktionselement	B	Hi	E	Beschreibung	B	Wert / Untere Bereichsgrenze	Obere Bereichsgrenze
Function definition with all types					*		
FPM_TEST_CHIP_PAGE_GAF|WDCA|R3TR (TADIR-Service)		+	-	FPM_TEST_CHIP_P...	*		
AAAB			-	Cross-application A...	*		
S_START		+	-	Start Authorization ...	*		
AUTHOBJNAM		C	-	Start Check: Object...	*	FPM_TEST_CHIP_PAGE_GAF	
AUTHOBJTYP		C	-	Start Check: Object...	*	WDCA	
AUTHPGMID		C	-	Start Check: Progra...	*	R3TR	
BC_Z			-	Basis - Central Func...	*		
S_PB_CHIP		+	-	ABAP Page Builder: ...	*		
ACTVT			-	Activity			
ACTVT			-	Create or generate		01	
ACTVT			-	Change		02	
ACTVT			-	Display		03	
CHIP_NAME		C	-	Web Dynpro ABAP:...	*	ID*	
S_PB_PAGE		+	-	ABAP Page Builder: ...	*		
ACTVT			-	Activity			
ACTVT			-	Create or generate		01,02,03	
CONFIG_ID		C	-	Configuration Ident...	*	$VariableName$	
CHIP_CATALOG_GET_LIST (RFC-Funktionsbaustein)		+	-	DE-EN-LANG-SWIT...	*		
AAAB			-	Cross-application A...	*		
S_RFC		+	-	Authorization Chec...	*		
ACTVT			-	Activity			
ACTVT			-	Execute		16	
RFC_NAME		C	-	Name (Whitelist) of ...	*	CHIP_CATALOG_GET_LIST	
RFC_TYPE		C	-	Type of RFC object...	*	FUNC	
BC_A			-	Basis: Administration	*		
S_CTS_ADMI		+	-	Administration Func...	*		
CTS_ADMFCT		C	-	Administration Task...	*	*	
S_CTS_SADM		+	-	System-Specific Ad...	*		
DESTSYS		C	-	Logical system	*	SYS[*]	
DOMAIN		C	-	TMS: Transport Do...	*	D01	D30
SE16 (Transaktion)		+	-	Data Browser	*		
AAAB			-	Cross-application A...	*		
S_TCODE		+	-	Transaction Code C...	*		
ACTVT			-	Activity			
TCD		C	-	Transaction Code	*	SE16	
HR			-	Human Resources	*		
P_TCODE		+	-	HR: Transaction co...	*		
TCD		C	-	Transaction Code	*	[*]	
SU01 (Transaktion)		+	-	User Maintenance	*		
AAAB			-	Cross-application A...	*		
S_TCODE		+	-	Transaction Code C...	*		
ACTVT			-	Activity			
TCD		C	-	Transaction Code	*	SU01	
BC_A			-	Basis: Administration	*		
S_USER_GRP		+	-	User Master Mainte...	*		
ACTVT			-	Activity			
ACTVT			-	Create or generate		01+02+03	
CLASS		C	-	User group in user ...	*	SUPER+AK_GR	

Bei aktiviertem Konfigurationsparameter, also ohne Berücksichtigung der SAP Applikationen, werden durch die abgebildete SAP Funktion alle SAP Rollen und SAP Profile ermittelt, die folgende Berechtigungen besitzen:

Berechtigungsobjekt **S_PB_CHIP** mit
Funktionselement **ACTVT** mit mindestens einer der Ausprägung **01** ODER **02** ODER **03**
UND
Funktionselement **CHIP_NAME** mit einer Ausprägung, die mit den Zeichen **ID** startet

UND

Berechtigungsobjekt **S_PB_PAGE** mit
Funktionselement **ACTVT** mit mindestens einer der Ausprägung **01** ODER **02** ODER **03**
UND
Funktionselement **CONFIG_ID** mit der Ausprägung, die als Wert in der Variable **$VariableName$** festgelegt ist,

UND

Berechtigungsobjekt **S_CTS_ADMI** mit
Funktionselement **CTS_ADMFCT** mit einer beliebigen Ausprägung

UND

Berechtigungsobjekt **S_CTS_SADM** mit
Funktionselement **DESTSYS** mit mindestens der Ausprägung von genau **SYS***
UND
Funktionselement **DOMAIN** mit mindestens einer Ausprägung im Wertebereich **D01** bis **D30**

UND

Berechtigungsobjekt **P_TCODE** mit
Funktionselement **TCD** mit genau der Ausprägung ***

UND

Berechtigungsobjekt **S_USER_GRP** mit
Funktionselement **ACTVT** mit mindestens den Ausprägungen **01** UND **02** UND **03**
UND
Funktionselement **CLASS** mit mindestens der Ausprägung **SUPER** UND **AK_GR**

Bei deaktiviertem Konfigurationsparameter werden durch die abgebildete SAP Funktion alle SAP Rollen und SAP Profile ermittelt, welche die folgenden Berechtigungen besitzen. Die Auswertung auf Ebene der Funktionselemente ist identisch zur Auswertung mit aktiviertem Konfigurationsparameter und ist daher nicht nochmals dargestellt.

SAP Applikation **FPM_TEST_CHIP_PAGE_GAF** mit
Berechtigungsobjekt **S_START**
UND
Berechtigungsobjekt **S_PB_CHIP**
UND
Berechtigungsobjekt **S_PB_PAGE**

ODER

SAP Applikation **CHIP_CATALOG_GET_LIST** mit
Berechtigungsobjekt **S_RFC**
UND
Berechtigungsobjekt **S_CTS_ADMI**
UND
Berechtigungsobjekt **S_CTS_SADM**

ODER

SAP Applikation **SE16** mit
Berechtigungsobjekt **S_TCODE**
UND
Berechtigungsobjekt **P_TCODE**

ODER

SAP Applikation **SU01** mit
Berechtigungsobjekt **S_TCODE**
UND
Berechtigungsobjekt **S_USER_GRP**

Verwandte Themen

- Hinweise für die Berechtigungsdefinition auf Seite 18
- Beispiele für SAP Funktionen auf Seite 30
- Eigenschaften von Berechtigungsdefinitionen und ihren Werten auf Seite 18

Beispiele für SAP Funktionen

Wenn Sie eine Berechtigungsdefinition erstellen, überlegen Sie, welche Berechtigungskombinationen nicht zulässig sind. Sie können zwei Anwendungsfälle unterscheiden:

1. Es sollen alle SAP Rollen und Profile mit unzulässigen Berechtigungskombinationen ermittelt werden.

   Erstellen Sie eine SAP Funktion für die Berechtigungen, die nicht gemeinsam in einer SAP Rolle oder einem SAP Profil auftreten dürfen. Durch die Berechtigungsprüfung werden alle SAP Rollen und Profile gefunden, die in der Summe ihrer Berechtigungen diese unzulässige Berechtigungskombination haben.

2. Es sollen alle Identitäten ermittelt werden, die über ihre SAP Benutzerkonten unzulässige Berechtigungskombinationen besitzen.

   Erstellen Sie verschiedene SAP Funktionen für Berechtigungen, die in ihrer Kombination nicht zulässig sind. Erstellen Sie Complianceregeln, die diese SAP Funktionen kombinieren. Bei der Compliancеprüfung werden alle Identitäten gefunden, die über die Summe aller Berechtigungen ihrer SAP Benutzerkonten solche unzulässigen Berechtigungskombinationen auf sich vereinen.

Beispiel für Anwendungsfall 1

In einem Unternehmen wurden die Richtlinien für zulässige SAP Berechtigungen geändert. Nun muss überprüft werden, ob die bestehenden Berechtigungen den neuen Richtlinien entsprechen. SAP Rollen und Profile mit unzulässigen Berechtigungskombinationen müssen identifiziert werden, damit sie an die neuen Anforderungen angepasst werden können.

Für jede Berechtigungskombination, die nicht zulässig ist, wird eine SAP Funktion erstellt.

Tabelle 6: Beispiel für eine Berechtigungsdefinition

SAP Funktion	SAP Applikation	Berechtigungsobjekt	Feld	Wert
F-A	TR1	BO2	ACTVT	*
	TR1	BO2	CLASS	*
	TR1	BO3	ACTVT	01+02
	TR1	S_TCODE	TCD	TR1
	RF	BO5	ACTVT	*
	RF	BO5	RLTYP	R*
	RF	S_RFC	RFC_NAME	RF
F-B	TR1	BO3	ACTVT	*
	TR1	BO4	ACTVT	02,03,07
	TR1	BO4	CLASS	DEF[*]
	TR1	S_TCODE	TCD	TR1

Folgende SAP Profile sind vorhanden:

Tabelle 7: Definierte SAP Profile

SAP Profil	SAP Applikation	Berechtigungsobjekt	Feld	Wert
P1	TR1	BO1	ACTVT	*
	TR1	BO1	CLASS	*
	TR1	BO3	ACTVT	*
	TR1	BO4	ACTVT	01, 02
	TR1	BO4	CLASS	DEF*
	TR1	S_TCODE	TCD	TR1

SAP Profil	SAP Applikation	Berechtigungsobjekt	Feld	Wert
P2	TR1	BO2	ACTVT	*
	TR1	BO2	CLASS	*
	TR1	BO3	ACTVT	01
	TR1	S_TCODE	TCD	TR1
P3	TR1	BO3	ACTVT	01, 02
	TR1	BO4	CLASS	*
	TR1	BO4	ACTVT	03, 07
P4	RF	BO5	ACTVT	03
	RF	BO5	RLTYP	*
	RF	S_RFC	RFC_NAME	RF

Bei der Berechtigungsprüfung werden die SAP Profile ermittelt, welche die SAP Funktion treffen.

Ergebnisse der Berechtigungsprüfung: **TestWithoutTCD** ist deaktiviert

- SAP Funktion: F-A

  Getroffenes SAP Profil: P4

  Das Profil P4 hat alle in der SAP Applikation RF benannten Berechtigungsobjekte, Felder und Ausprägungen.

  Dem Profil P1 fehlen die Berechtigungsobjekte BO2, S_TCODE, BO5 und S_RFC. Daher trifft es die SAP Funktion nicht.

  Dem Profil P2 fehlen die Ausprägung 02 für das Berechtigungsobjekt BO3 sowie die Berechtigungsobjekte BO5 und S_RFC. Daher trifft es die SAP Funktion nicht.

  Dem Profil P3 fehlen die Berechtigungsobjekte BO2, S_TCODE, BO5 und S_RFC. Daher trifft es die SAP Funktion nicht.

- SAP Funktion: F-B

  Getroffenes SAP Profil: P1

  Das Profil P1 hat alle in der SAP Funktion benannten Berechtigungsobjekte und Felder sowie mindestens eine der Ausprägungen.

  Dem Profil P2 fehlt das Berechtigungsobjekt BO4. Daher trifft es die SAP Funktion nicht.

  Dem Profil P3 fehlt das Berechtigungsobjekt S_TCODE. Daher trifft es die SAP Funktion nicht.

  Dem Profil P4 fehlen die Berechtigungsobjekte BO3, BO4 und S_TCODE. Daher trifft es die SAP Funktion nicht.

Wenn für die Berechtigungsprüfung der Konfigurationsparameter **TestWithoutTCD** deaktiviert ist, dann entsprechen die SAP Profile P2 und P3 den neuen Richtlinien und können daher weiter genutzt werden. Die Profile P1 und P4 müssen den neuen Richtlinien angepasst werden.

Ergebnisse der Berechtigungsprüfung: **TestWithoutTCD** ist aktiviert

- SAP Funktion: F-A

  Die Berechtigungsobjekte S_TCODE und S_RFC werden bei der Prüfung ignoriert.

  Getroffene SAP Profile: keine

  Dem Profil P1 fehlen die Berechtigungsobjekte BO2 und BO5. Daher trifft es die SAP Funktion nicht.

  Dem Profil P2 fehlen das Berechtigungsobjekt BO5 und die Ausprägung 02 für das Berechtigungsobjekt BO3. Daher trifft es die SAP Funktion nicht.

  Dem Profil P3 fehlen die Berechtigungsobjekte BO2 und BO5. Daher trifft es die SAP Funktion nicht.

  Dem Profil P4 fehlen die Berechtigungsobjekte BO2 und BO3. Daher trifft es die SAP Funktion nicht.

- SAP Funktion: F-B

  Das Berechtigungsobjekt S_TCODE wird bei der Prüfung ignoriert.

  Getroffene SAP Profile: P1, P3

  Das Profil P1 hat alle in der SAP Funktion benannten Berechtigungsobjekte und Felder sowie mindestens eine der Ausprägungen.

  Das Profil P3 hat alle in der SAP Funktion benannten Berechtigungsobjekte und Felder sowie mindestens eine der Ausprägungen.

  Dem Profil P2 fehlt das Berechtigungsobjekt BO4. Daher trifft es die SAP Funktion nicht.

  Dem Profil P4 fehlen die Berechtigungsobjekte BO3 und BO4. Daher trifft es die SAP Funktion nicht.

Wenn für die Berechtigungsprüfung der Konfigurationsparameter **TestWithoutTCD** aktiviert ist, dann entsprechen die SAP Profile P2 und P4 den neuen Richtlinien und können weiter genutzt werden. Die Profile P1 und P3 müssen angepasst werden.

Beispiel für Anwendungsfall 2

Es soll geprüft werden, welche SAP Benutzerkonten den Richtlinien widersprechen. Folgende Benutzerkonten und Identitäten sind vorhanden:

- User A mit Benutzerkonto K1 mit dem SAP Profil P1
- User B mit Benutzerkonto K2 mit den SAP Profilen P2 und P3
- User C mit Benutzerkonto K3 mit dem SAP Profil P2 und Benutzerkonto K4 mit dem SAP Profil P3

Die SAP Profile haben folgende Berechtigungen:

- P1 mit BO1 und BO2
- P2 mit BO1
- P3 mit BO2

Eine Identität darf nicht gleichzeitig die Berechtigungen BO1 und BO2 besitzen. Zur Prüfung wird die SAP Funktion SF-A erstellt. Eine Complianceregel CR-X ermittelt alle Identitäten, welche diese SAP Funktion treffen.

- SF-A prüft BO1 UND BO2
- CR-X: Die Identität besitzt mindestens die SAP Funktion SF-A.

Nur das SAP Profil P1 trifft die SAP Funktion. Damit ermittelt die Complianceregel nur für User A eine Regelverletzung. Damit auch die Kombination der SAP Profile P2 und P3 als unzulässig erkannt wird, müssen weitere SAP Funktionen und Complianceregeln erstellt werden.

- SF-B prüft BO1
- SF-C prüft BO2
- CR-Y: Die Identität besitzt mindestens die SAP Funktion SF-B UND die Identität besitzt mindestens die SAP Funktion SF-C.

Die SAP Profile P1 und P2 treffen die SAP Funktion SF-B. Die SAP Profile P1 und P3 treffen die SAP Funktion SF-C. Somit können durch die Complianceregel CR-Y alle Identitäten ermittelt werden, denen über ihre Benutzerkonten die SAP Profile P1 oder P2 und P3 zugewiesen sind und die dadurch beide Berechtigungen BO1 und BO2 besitzen.

Tabelle 8: Ergebnis der Regelprüfung

Regel	Regelbedingung	Identitäten, welche die Regeln verletzen
CR-X	Die Identität besitzt mindestens die SAP Funktion SF-A.	User A
CR-Y	Die Identität besitzt mindestens die SAP Funktion SF-B UND die Identität besitzt mindestens die SAP Funktion SF-C.	User A User B User C

Verwandte Themen

- Ermitteln unzulässiger Berechtigungen auf Seite 24
- Regelbedingungen für SAP Funktionen auf Seite 56

Funktionsdefinitionen bearbeiten

Für jede Funktionsdefinition wird in der Datenbank eine Arbeitskopie angelegt. Um Funktionsdefinitionen zu ändern, bearbeiten Sie deren Arbeitskopien. Erst mit Aktivierung der Arbeitskopie werden die Änderungen auf die produktive Funktionsdefinition übertragen. SAP Berechtigungen werden nur anhand aktivierter Funktionsdefinitionen überprüft.

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

Um eine bestehende Funktionsdefinition zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Funktionsdefinitionen**.
   a. Wählen Sie in der Ergebnisliste eine Funktionsdefinition.
   b. Wählen Sie die Aufgabe **Arbeitskopie erstellen**.

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

   - ODER -

   Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Arbeitskopien von Funktionsdefinitionen**.
   a. Wählen Sie in der Ergebnisliste eine Arbeitskopie.
   b. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
2. Bearbeiten Sie die Stammdaten der Arbeitskopie.
3. Speichern Sie die Änderungen.
4. Wählen Sie die Aufgabe **Arbeitskopie aktivieren** und bestätigen Sie die Sicherheitsabfrage mit **OK**.

   Die Änderungen an der Arbeitskopie werden auf die aktive Funktionsdefinition übertragen.

Verwandte Themen

- Arbeitskopien erstellen auf Seite 37
- Allgemeine Stammdaten einer Funktionsdefinition auf Seite 15
- Arbeitskopien aktivieren auf Seite 23

Überblick über Funktionsdefinitionen

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

Um einen Überblick über eine Funktionsdefinition zu erhalten

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Funktionsdefinitionen**.
2. Wählen Sie in der Ergebnisliste die Funktionsdefinition.
3. Wählen Sie die Aufgabe **Überblick über die Funktionsdefinition**.

Um einen Überblick über eine Arbeitskopie zu erhalten

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Arbeitskopien von Funktionsdefinitionen**.
2. Wählen Sie in der Ergebnisliste die Funktionsdefinition.
3. Wählen Sie die Aufgabe **Überblick über die Funktionsdefinition**.

Berechtigungsübersicht

In der Berechtigungsübersicht werden die Funktionselemente in einer flachen Struktur dargestellt.

Um eine Übersicht aller Funktionselemente für eine aktive Funktionsdefinition anzuzeigen

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Funktionsdefinitionen**.
2. Wählen Sie in der Ergebnisliste die Funktionsdefinition.
3. Wählen Sie die Aufgabe **Berechtigungsübersicht**.

Um eine Übersicht aller Funktionselemente für eine Arbeitskopie anzuzeigen

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Arbeitskopien von Funktionsdefinitionen**.
2. Wählen Sie in der Ergebnisliste die Funktionsdefinition.
3. Wählen Sie die Aufgabe **Berechtigungsübersicht**.

   Sie können hier alle Objekteigenschaften bearbeiten.

Verwandte Themen

- Berechtigungsdefinitionen im Berechtigungseditor erstellen auf Seite 17

Arbeitskopien erstellen

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

Um eine Arbeitskopie zu erstellen

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

Verwandte Themen

- Arbeitskopien aktivieren auf Seite 23

Funktionsdefinitionen exportieren

Um SAP Funktionen beispielsweise aus einer Entwicklungsumgebung in eine Produktivdatenbank zu übernehmen, können die Funktionsdefinitionen in CSV-Dateien exportiert werden. Diese CSV-Dateien können in andere Datenbanken importiert werden.

Um eine Funktionsdefinition in eine CSV-Datei zu exportieren

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Funktionsdefinitionen**.
2. Wählen Sie in der Ergebnisliste die Funktionsdefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Exportieren**.
5. Legen Sie den Dateinamen und Speicherort für die CSV-Datei fest.
6. Klicken Sie **Speichern**.

Folgende Eigenschaften werden exportiert:

Tabelle 9: Exportierte Stammdaten einer Funktionsdefinition

Eigenschaft	Datenfeld in der CSV-Datei
Name der Funktionsdefinition	Function
zugeordnete Funktionskategorie	Process

Eigenschaft	Datenfeld in der CSV-Datei
Beschreibung	Function Description
Auswirkung	Risk Level
Berechtigungsvorschlagswert	TransactionType
Transaktionscode	Transaction
TADIR-Programm-ID	AUTHPGMID
TADIR-Objekttyp	AUTHOBJTYP
TADIR-Objektname	AUTHOBJNAM
Typ des externen Services	SRV_TYPE
Name des externen Services	SRV_NAME
RFC-Objekttyp	RFC_TYPE
RFC-Objektname	RFC_NAME
Hashwert	SAPHashValue
Berechtigungsobjekte	Object
Berechtigungsfelder	Field
Beschreibung der Berechtigungsfelder	Field Description
Wert/Untere Bereichsgrenze	Value From
Obere Bereichsgrenze	Value To

Zu jedem Datensatz wird in der CSV-Datei eine zusätzliche Information zum Importstatus (`State`) geführt. Der Importstatus wird beim Export standardmäßig auf **1** gesetzt. Diese Information wird beim Import von Funktionsdefinitionen ausgewertet.

Verwandte Themen

- Funktionsdefinitionen importieren auf Seite 53
- Arbeitskopien exportieren auf Seite 38
- Alle Funktionsdefinitionen exportieren auf Seite 52

Arbeitskopien exportieren

Um SAP Funktionen beispielsweise aus einer Entwicklungsumgebung in eine Produktivdatenbank zu übernehmen, können die Funktionsdefinitionen in CSV-Dateien exportiert werden. Diese CSV-Dateien können in andere Datenbanken importiert werden.

Um die Funktionsdefinition einer Arbeitskopie in eine CSV-Datei zu exportieren

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Arbeitskopien von Funktionsdefinitionen**.
2. Wählen Sie in der Ergebnisliste die Funktionsdefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Exportieren**.
5. Legen Sie den Dateinamen und Speicherort für die CSV-Datei fest.
6. Klicken Sie **Speichern**.

Folgende Eigenschaften werden exportiert:

Tabelle 10: Exportierte Stammdaten einer Funktionsdefinition

Eigenschaft	Datenfeld in der CSV-Datei
Name der Funktionsdefinition	Function
zugeordnete Funktionskategorie	Process
Beschreibung	Function Description
Auswirkung	Risk Level
Berechtigungsvorschlagswert	TransactionType
Transaktionscode	Transaction
TADIR-Programm-ID	AUTHPGMID
TADIR-Objekttyp	AUTHOBJTYP
TADIR-Objektname	AUTHOBJNAM
Typ des externen Services	SRV_TYPE
Name des externen Services	SRV_NAME
RFC-Objekttyp	RFC_TYPE
RFC-Objektname	RFC_NAME
Hashwert	SAPHashValue
Berechtigungsobjekte	Object
Berechtigungsfelder	Field
Beschreibung der Berechtigungsfelder	Field Description
Wert/Untere Bereichsgrenze	Value From
Obere Bereichsgrenze	Value To

Zu jedem Datensatz wird in der CSV-Datei eine zusätzliche Information zum Importstatus (`State`) geführt. Der Importstatus wird beim Export standardmäßig auf **1** gesetzt. Diese Information wird beim Import von Funktionsdefinitionen ausgewertet.

Verwandte Themen

- Funktionsdefinitionen importieren auf Seite 53
- Funktionsdefinitionen exportieren auf Seite 37
- Alle Funktionsdefinitionen exportieren auf Seite 52

Funktionsausprägungen definieren

Ein und dieselbe Funktionsdefinition kann für verschiedene konkrete Ausprägungen genutzt werden. In Funktionsausprägungen wird ein konkreter SAP Mandant angegeben, in dem die SAP Funktion angewendet wird. Des Weiteren werden die Variablen, die den Berechtigungsfeldern zugeordnet sind, mit konkreten Werten versehen. Funktionsausprägungen können nur für aktivierte SAP Funktionen erstellt werden.

Um eine Funktionsausprägung zu erstellen

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Funktionsausprägungen**.
2. Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Funktionsausprägung.
4. Speichern Sie die Änderungen.

Um eine Funktionsausprägung zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Funktionsausprägungen**.
2. Wählen Sie in der Ergebnisliste eine Funktionsausprägung und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten der Funktionsausprägung.
4. Speichern Sie die Änderungen.

HINWEIS: One Identity Manager Benutzer mit der Anwendungsrolle **Identity & Access Governance | Identity Audit | Pflege SAP Funktionen** können Funktionsausprägungen für die SAP Funktionen erstellen und bearbeiten, für die sie als Verantwortliche eingetragen sind.

Detaillierte Informationen zum Thema

- Stammdaten von Funktionsausprägungen auf Seite 41
- Definition der Feldvariablen prüfen auf Seite 42

- Überblick über die Funktionsausprägung auf Seite 42

Stammdaten von Funktionsausprägungen

Für eine Funktionsausprägung erfassen Sie folgende Stammdaten.

Tabelle 11: Eigenschaften einer Funktionsausprägung

Eigenschaft	Beschreibung
Funktionsdefinition	Funktionsdefinition, für welche die Funktionsausprägung erstellt werden soll.
Mandant	SAP Mandant, auf den die SAP Funktion angewendet werden soll.
Variablenset	Variablenset, in dem die Variablen definiert sind, die in der Funktionsdefinition verwendet werden. Dem Variablenset und der Funktionsausprägung muss derselbe SAP Mandant zugeordnet sein.
Verantwortliche	Anwendungsrolle, deren Mitglieder inhaltlich für diese Funktionsausprägung und Variablensets verantwortlich sind. Um eine neue Anwendungsrolle zu erstellen, klicken Sie . Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle zu.
Anzeigename	Anzeigename der Funktionsausprägung. Er wird per Bildungsregel aus der Bezeichnung der Funktionsdefinition, dem zugeordneten Mandanten und dem zugeordneten Variablenset gebildet.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen. Für eine neue Funktionsausprägung wird Beschreibung der Funktionsdefinition übernommen.
Funktionsausprägungselemente	Abbildung der SAP Applikationen, Berechtigungsobjekte und Funktionselemente der SAP Funktion mit den konkreten Werten, die aus dem zugeordneten Variablenset ermittelt werden. Änderungen an den Variablen oder am Variablenset werden angezeigt, sobald der DBQueue Prozessor die zugehörigen Berechnungsaufträge abgearbeitet hat.

Verwandte Themen

- Variablensets für Berechtigungsdefinitionen erstellen und bearbeiten auf Seite 43
- Pflege von SAP Funktionen auf Seite 51
- Definition der Feldvariablen prüfen auf Seite 42

Definition der Feldvariablen prüfen

Bevor Sie Funktionsausprägungen in Complianceregeln verwenden, prüfen Sie, ob alle Variablen, die in der Funktionsdefinition verwendet werden, im zugeordneten Variablenset definiert sind. Wenn der Funktionsausprägung keine Funktionsdefinition oder kein Variablenset zugeordnet ist, wird die Prüfung mit einer Fehlermeldung abgebrochen. Wenn einzelne Variablen nicht im zugeordneten Variablenset definiert sind, werden diese in der Fehlermeldung aufgelistet.

Um die Definition der Feldvariablen zu prüfen

1. Wählen Sie im Manager die Kategorie **Identity Audit>| SAP Funktionen > Funktionsausprägungen**.
2. Wählen Sie in der Ergebnisliste die Funktionsausprägung.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Definition der Feldvariablen prüfen**.

Verwandte Themen

- Stammdaten von Funktionsausprägungen auf Seite 41
- Stammdaten eines Variablensets auf Seite 43

Überblick über die Funktionsausprägung

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

Um einen Überblick über eine Funktionsausprägung zu erhalten

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Funktionsausprägungen**.
2. Wählen Sie in der Ergebnisliste die Funktionsausprägung.
3. Wählen Sie die Aufgabe **Überblick über die Funktionsausprägung**.

Variablensets für Berechtigungsdefinitionen erstellen und bearbeiten

In einem Variablenset stellen Sie alle Variablen zusammen, die in einer Berechtigungsdefinition verwendet werden, und ordnen ihnen konkrete Werte zu.

Um ein Variablenset zu erstellen

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Variablensets**.
2. Klicken Sie in der Ergebnisliste  .
3. Bearbeiten Sie die Stammdaten des Variablensets.
4. Speichern Sie die Änderungen.

Um ein Variablenset zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Variablensets**.
2. Wählen Sie in der Ergebnisliste ein Variablenset und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten des Variablensets.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Stammdaten eines Variablensets auf Seite 43
- In SAP Funktionen verwendete Variablen übernehmen auf Seite 45

Verwandte Themen

- Berechtigungsdefinitionen im Berechtigungseditor erstellen auf Seite 17
- Überblick über ein Variablenset auf Seite 46
- Variablensets kopieren auf Seite 45

Stammdaten eines Variablensets

Für Variablensets erfassen Sie folgende Stammdaten.

Tabelle 12: Stammdaten eines Variablensets

Eigenschaft	Beschreibung
Variablenset	Eindeutige Bezeichnung des Variablensets.
Mandant	SAP Mandant, für den das Variablenset gelten soll.
Abteilung	Abteilung, für die das Variablenset relevant ist.
Unternehmensbereich	Unternehmensbereich, für den das Variablenset relevant ist.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
SAP Feldvariablen	Liste der definierten Variablen.

Um eine Feldvariable im Variablenset anzulegen

- Klicken Sie **Hinzufügen** und erfassen Sie die folgenden Eigenschaften.
  - **Variable**: Namen der Variable in der Notation `${alphanum}+$`.

    HINWEIS: Variablennamen dürfen nicht mit dem Namen von Systemvariablen beginnen. Variablensets mit solchen Variablen können nicht gespeichert werden.
  - **Wert**: Konkrete Ausprägungen für die Variable, die in die Funktionsausprägung übernommen werden sollen.
  - **Beschreibung**: Freitextfeld für zusätzliche Erläuterungen.
  - **Berechtigungsobjekt**: Verweis auf das Berechtigungsobjekt, in dem die Variable angewendet werden soll.

  Auf dem Formular steht Ihnen eine Auswahlhilfe zur Verfügung. Sie können hier die zu einem Berechtigungsobjekt vorhandenen Berechtigungsfelder auswählen und für die Definition von Variablen nutzen.

Um eine Feldvariable aus dem Variablenset zu löschen

1. Markieren Sie eine Zeile in der Liste der Feldvariablen.
2. Klicken Sie **Ausgewählte entfernen**.

TIPP: Sie können Variablensets anlegen ohne Variablen zu definieren. Nutzen Sie diese Variablensets für Funktionsdefinitionen, in denen keine Variablen als Werte eingetragen sind.

Detaillierte Informationen zum Thema

- Verwenden von Variablen auf Seite 21

Verwandte Themen

- In SAP Funktionen verwendete Variablen übernehmen auf Seite 45

In SAP Funktionen verwendete Variablen übernehmen

Variablen, die in den Berechtigungsdefinitionen von SAP Funktionen verwendet werden, können in Variablensets übernommen werden.

Um Variablen in ein Variablenset zu übernehmen

1. Wählen Sie die Kategorie **Identity Audit > SAP Funktionen > Variablensets**.
2. Wählen Sie in der Ergebnisliste das Variablenset.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Verwendete Variablen übernehmen**.
5. Markieren Sie alle Funktionsdefinitionen oder Arbeitskopien, aus denen die Variablen in das Variablenset übernommen werden sollen.

   Mehrfachauswahl ist möglich.
6. Klicken Sie **OK**, um die Variablen zu übernehmen.

   Alle Variablen aus den ausgewählten Funktionsdefinitionen werden in die Liste der Feldvariablen eingefügt.
7. Bearbeiten Sie die Eigenschaften der Variablen.
8. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten eines Variablensets auf Seite 43

Variablensets kopieren

Um ein Variablenset zu kopieren

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Variablensets**.
2. Wählen Sie in der Ergebnisliste das Variablenset und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Wählen Sie die Aufgabe **Variablenset kopieren**.
4. Um die Stammdaten der Kopie sofort zu bearbeiten, klicken Sie **Ja**.
5. Bearbeiten Sie die Stammdaten der Kopie.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten eines Variablensets auf Seite 43

Überblick über ein Variablenset

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

Um einen Überblick über ein Variablenset zu erhalten

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Variablensets**.
2. Wählen Sie in der Ergebnisliste das Variablenset.
3. Wählen Sie die Aufgabe **Überblick über das Variablenset**.

Risikomindernde Maßnahmen an SAP Funktionen zuweisen

An SAP Funktionen können risikomindernde Maßnahmen hinterlegt werden. Durch diese sollen die Auswirkungen gesenkt werden, die für ein Unternehmen entstehen, wenn SAP Benutzerkonten die SAP Funktion treffen. Dabei legen Sie fest, wie mit SAP Benutzerkonten oder SAP Gruppen verfahren werden soll, die die SAP Funktion treffen. So kann beispielsweise die Änderung der Benutzerzuordnung zu einer SAP Rolle im SAP System eine geeignete risikomindernde Maßnahme für eine SAP Funktion darstellen.

Risikomindernde Maßnahmen können auch als Kontrollmaßnahmen für Complianceregeln erstellt werden. In Complianceregeln über SAP Funktionen werden automatisch die risikomindernden Maßnahmen übernommen, die den zu prüfenden SAP Funktionen zugewiesen sind.

Voraussetzungen:

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

Um risikomindernde Maßnahmen zu bearbeiten

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

Detaillierte Informationen zum Thema

- Risikomindernde Maßnahmen an Funktionsdefinitionen zuweisen auf Seite 47
- Risikomindernde Maßnahmen für SAP Funktionen erstellen auf Seite 47
- Risikomindernde Maßnahmen für SAP Funktionen auf Seite 60

Risikomindernde Maßnahmen an Funktionsdefinitionen zuweisen

Um risikomindernde Maßnahmen an eine Funktionsdefinition zuzuweisen

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Arbeitskopien von Funktionsdefinitionen**.
2. Wählen Sie in der Ergebnisliste die Arbeitskopie.
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 für SAP Funktionen erstellen

Um eine risikomindernde Maßnahme für SAP Funktionen zu erstellen

1. Wählen Sie im Manager die Kategorie **Identity Audit > SAP Funktionen > Arbeitskopien von Funktionsdefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Arbeitskopie.
3. Wählen Sie die Aufgabe **Risikomindernde Maßnahmen zuweisen**.
4. Wählen Sie die Aufgabe **Risikomindernde Maßnahme erstellen**.
5. Erfassen Sie die Stammdaten der risikomindernden Maßnahme.
6. Speichern Sie die Änderungen.
7. Wählen Sie die Aufgabe **Funktionsdefinitionen zuweisen**.

8. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die Funktionsdefinitionen, die zugewiesen werden sollen.
9. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Risikomindernde Maßnahmen für SAP Funktionen auf Seite 60

Basisdaten für SAP Funktionen

Für SAP Funktionen sind folgende Basisdaten relevant:

- SAP Funktionskategorien

  SAP Funktionskategorien verwenden Sie um SAP Funktionen nach spezifischen Kriterien zu gruppieren.

  Weitere Informationen finden Sie unter SAP Funktionskategorien auf Seite 48.
- Unternehmensbereiche

  Unternehmensbereiche können als zusätzliches Gruppierungsmerkmal für SAP Funktionen genutzt werden. Darüber hinaus können Sie Unternehmensbereiche nutzen, um Regelverletzungen im Rahmen des Identity Audit für verschiedene SAP Funktionen auszuwerten und um Bestellungen im IT Shop oder Attestierungsvorgänge per Peer-Gruppen-Analyse zu entscheiden.

  Weitere Informationen finden Sie unter Unternehmensbereiche auf Seite 49.
- Pflege SAP Funktionen

  An SAP Funktionen können Identitäten zugewiesen werden, die inhaltlich für diese SAP Funktionen verantwortlich sind und damit die Arbeitskopien bearbeiten können.

  Weitere Informationen finden Sie unter Pflege von SAP Funktionen auf Seite 51.

SAP Funktionskategorien

Funktionskategorien verwenden Sie um SAP Funktionen nach spezifischen Kriterien zu gruppieren.

Um eine Funktionskategorie zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Identity Audit > Basisdaten zur Konfiguration > SAP Funktionskategorien**.
2. Wählen Sie in der Ergebnisliste eine Funktionskategorie und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

Klicken Sie in der Ergebnisliste .

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

Für eine Funktionskategorie erfassen Sie folgende Stammdaten.

Tabelle 13: Eigenschaften einer SAP Funktionskategorie

Eigenschaft	Beschreibung
Kategorie	Bezeichnung der Funktionskategorie.
Übergeordnete Kategorie	Übergeordnete Funktionskategorie, um Funktionskategorien hierarchisch zu organisieren.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Verwandte Themen

- Allgemeine Stammdaten einer Funktionsdefinition auf Seite 15

Unternehmensbereiche

Unternehmensbereiche können Sie nutzen, um Regelverletzungen im Rahmen des Identity Audit für verschiedene SAP Funktionen auszuwerten. Für Unternehmensbereiche und SAP Funktionen können Sie Kriterien erfassen, die Auskunft über das Risiko von Regelverletzungen geben.

Um Regelprüfungen im Rahmen des Identity Audit für verschiedene Bereiche Ihres Unternehmens auswerten zu können, richten Sie Unternehmensbereiche ein. Unternehmensbereiche können an hierarchische Rollen und Leistungspositionen zugeordnet werden. Für die Unternehmensbereiche und die hierarchischen Rollen können Sie Kriterien erfassen, die Auskunft über das Risiko von Regelverletzungen geben. Dafür legen Sie fest, wie viele Regelverletzungen in einem Unternehmensbereich oder einer Rolle zulässig sind. Für jede Rolle können Sie separate Bewertungskriterien erfassen, wie beispielsweise Risikoindex oder Transparenzindex.

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

Beispiel: Einsatz von Unternehmensbereichen

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

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

Um Unternehmensbereiche zu erstellen oder zu bearbeiten

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

   - ODER -

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

Für einen Unternehmensbereich erfassen Sie folgende Stammdaten.

Tabelle 14: Eigenschaften von Unternehmensbereichen

Eigenschaft	Beschreibung
Unternehmensbereich	Bezeichnung des Unternehmensbereichs.
Überg. Unternehmensbereich	Übergeordneter Unternehmensbereich in einer Hierarchie. Wählen Sie aus der Auswahlliste den übergeordneten Unternehmensbereich aus, um Unternehmensbereiche hierarchisch zu organisieren.
Max. Anzahl Regelverletzungen	Anzahl der Regelverletzungen, die in diesem Unternehmensbereich zulässig sind. Dieser Wert kann bei der Regelprüfung ausgewertet werden.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

In Regeln über SAP Funktionen werden automatisch die risikomindernden Maßnahmen übernommen, die den zu prüfenden Funktionsdefinitionen zugewiesen sind. Die Bedingungen dafür sind:

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

Verwandte Themen

- Risikomindernde Maßnahmen für SAP Funktionen auf Seite 60
- Allgemeine Stammdaten einer Funktionsdefinition auf Seite 15

Pflege von SAP Funktionen

An SAP Funktionen können Identitäten zugewiesen werden, die inhaltlich für diese SAP Funktionen verantwortlich sind. Dazu ordnen Sie den Funktionsdefinitionen eine Anwendungsrolle für die Pflege von SAP Funktionen zu. Dieser Anwendungsrolle weisen Sie die Identitäten zu, die berechtigt sind, die Arbeitskopie dieser Funktionsdefinition zu bearbeiten, zu aktivieren und Funktionsausprägungen zu definieren.

Im One Identity Manager ist eine Standardanwendungsrolle für die Pflege von SAP Funktionen vorhanden. Bei Bedarf erstellen Sie weitere Anwendungsrollen. Ausführliche Informationen zum Einsatz und zur Bearbeitung von Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Tabelle 15: Standardanwendungsrolle für die Pflege von SAP Funktionen

Benutzer	Aufgaben
Verantwortliche für die Pflege der SAP Funktionen	Die Administratoren müssen der Anwendungsrolle **Identity & Access Governance | Identity Audit | Pflege SAP Funktionen** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Sind inhaltlich für die SAP Funktionen verantwortlich. • Bearbeiten die Arbeitskopien der Funktionsdefinitionen, für die sie verantwortlich sind. • Definieren die Funktionsausprägungen und Variablensets für SAP Funktionen. • Weisen risikomindernde Maßnahmen zu.

Um Identitäten in die Standardanwendungsrolle für die Pflege von SAP Funktionen aufzunehmen

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

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Identität und doppelklicken Sie .

4. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten einer Funktionsdefinition auf Seite 15

Alle Funktionsdefinitionen exportieren

Um SAP Funktionen beispielsweise aus einer Entwicklungsumgebung in eine Produktivdatenbank zu übernehmen, können die Funktionsdefinitionen in CSV-Dateien exportiert werden. Diese CSV-Dateien können in andere Datenbanken importiert werden.

Um alle Funktionsdefinitionen in eine CSV-Datei zu exportieren

1. Wählen Sie im Manager die Kategorie **Identity Audit**.
2. Wählen Sie das Menü **Plugins > Alle SAP Funktionsdefinitionen exportieren**.
3. Um nur die Arbeitskopien zu exportieren, klicken Sie **Ja**.

   - ODER -

   Um nur die aktivierten SAP Funktionen zu exportieren, klicken Sie **Nein**.
4. Legen Sie den Dateinamen und Speicherort für die CSV-Datei fest.
5. Klicken Sie **Speichern**.

   Es werden alle Funktionsdefinitionen fortlaufend in die Datei geschrieben.

Folgende Eigenschaften werden exportiert:

Tabelle 16: Exportierte Stammdaten einer Funktionsdefinition

Eigenschaft	Datenfeld in der CSV-Datei
Name der Funktionsdefinition	Function
zugeordnete Funktionskategorie	Process
Beschreibung	Function Description
Auswirkung	Risk Level
Berechtigungsvorschlagswert	TransactionType
Transaktionscode	Transaction

Eigenschaft	Datenfeld in der CSV-Datei
TADIR-Programm-ID	AUTHPGMID
TADIR-Objekttyp	AUTHOBJTYP
TADIR-Objektname	AUTHOBJNAM
Typ des externen Services	SRV_TYPE
Name des externen Services	SRV_NAME
RFC-Objekttyp	RFC_TYPE
RFC-Objektname	RFC_NAME
Hashwert	SAPHashValue
Berechtigungsobjekte	Object
Berechtigungsfelder	Field
Beschreibung der Berechtigungsfelder	Field Description
Wert/Untere Bereichsgrenze	Value From
Obere Bereichsgrenze	Value To

Zu jedem Datensatz wird in der CSV-Datei eine zusätzliche Information zum Importstatus (`State`) geführt. Der Importstatus wird beim Export standardmäßig auf **1** gesetzt. Diese Information wird beim Import von Funktionsdefinitionen ausgewertet.

HINWEIS: Verantwortliche für die Pflege der SAP Funktionen können nur die Funktionsdefinitionen exportieren, für die sie als Verantwortliche in den Stammdaten eingetragen sind.

Verwandte Themen

- Funktionsdefinitionen importieren auf Seite 53
- Arbeitskopien exportieren auf Seite 38
- Funktionsdefinitionen exportieren auf Seite 37

Funktionsdefinitionen importieren

Um SAP Funktionen beispielsweise aus einer Entwicklungsumgebung in eine Produktivdatenbank zu übernehmen, können die Funktionsdefinitionen in CSV-Dateien exportiert werden. Diese CSV-Dateien können in andere Datenbanken importiert werden.

Beim Import von SAP Funktionen aus einer vorhandenen CSV-Datei werden die in der CSV-Datei enthaltenen Funktionsdefinitionen als Arbeitskopien in die Datenbank übertragen. Damit Funktionsdefinitionen importiert werden können, müssen folgende Datenfelder in der CSV-Datei vorhanden sein.

Tabelle 17: Datenfelder für den Import von Funktionsdefinitionen

Datenfeld in der CSV-Datei (Kopfzeile)	Objekteigenschaft im One Identity Manager
Function	Funktionsdefinition
TransactionType	Berechtigungsvorschlagswert
Object	Berechtigungsobjekt
Field	Berechtigungsfeld
Value From	Wert/Untere Bereichsgrenze
Value To	Obere Bereichsgrenze
State	Keine Entsprechung. Über den Importstatus wird geregelt, welche Datensätze in den One Identity Manager importiert werden sollen. **1**: importieren
Process (optional)	Kategorie
Function Description (optional)	Beschreibung der Funktionsdefinition.
Risk Level (optional)	Auswirkung Mögliche Werte sind {**Low**|**Medium**|**High**|**Critical**}.
Transaction (optional)	Transaktionscode
AUTHPGMID (optional)	TADIR-Programm-ID
AUTHOBJTYP (optional)	TADIR-Objekttyp
AUTHOBJNAM (optional)	TADIR-Objektname
SRV_TYPE (optional)	Type des externen Services
SRV_NAME (optional)	Name des externen Services
RFC_TYPE (optional)	RFC-Objekttyp
RFC_NAME	RFC-Objektname

Datenfeld in der CSV-Datei (Kopfzeile)	Objekteigenschaft im One Identity Manager
(optional)	
SAPHashValue (optional)	Hashwert
Field Description (optional)	Beschreibung der Berechtigungsfelder, Berechtigungsobjekte und SAP Applikationen.

HINWEIS:

- Die Reihenfolge der Datenfelder ist beliebig.
- Alle benötigten Datenfelder müssen in der Kopfzeile definiert und in den Datensätzen vorhanden sein.
- Datenfelder ohne Wert sind durch zwei aufeinanderfolgende Trennzeichen zu kennzeichnen.
- Datensätze mit fehlenden Pflichtfeldern werden nicht importiert.

Um Funktionsdefinitionen zu importieren

1. Wählen Sie im Manager die Kategorie **Identity Audit**.
2. Wählen Sie das Menü **Plugins > SAP Funktionsdefinitionen Import**.
3. Wählen Sie die zu importierende CSV-Datei und klicken Sie **Öffnen**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Es werden alle Funktionsdefinitionen als Arbeitskopien in die Datenbank übertragen. Wenn bereits eine Arbeitskopie mit gleichem Namen in der Datenbank vorhanden ist, wird diese durch den Import überschrieben.

Verwandte Themen

- Alle Funktionsdefinitionen exportieren auf Seite 52
- Arbeitskopien exportieren auf Seite 38
- Funktionsdefinitionen exportieren auf Seite 37

4

Complianceregeln für SAP Funktionen

Neben den Berechtigungen, die eine Identität in einem SAP R/3 System aufgrund ihrer Benutzerkonten und Gruppen- und Rollenmitgliedschaften haben kann, können auch die effektiven Bearbeitungsrechte durch Complianceregeln überprüft werden. Effektive Bearbeitungsrechte werden über SAP Funktionen geprüft. Dafür werden die SAP Funktionen in Regelbedingungen aufgenommen.

Bei der Regelprüfung wird der Gültigkeitszeitraum von Rollenzuweisungen berücksichtigt.

Ausführliche Informationen über Complianceregeln finden Sie im *One Identity Manager Administrationshandbuch für Complianceregeln*.

Detaillierte Informationen zum Thema

- Regelbedingungen für SAP Funktionen auf Seite 56
- Risikomindernde Maßnahmen für Complianceregeln mit SAP Funktionen auf Seite 58

Regelbedingungen für SAP Funktionen

Um eine neue Regel für SAP Funktionen zu definieren

1. Wählen Sie im Manager die Kategorie **Identity Audit > Regeln**.
2. Klicken Sie in der Ergebnisliste .
3. Erfassen Sie die Stammdaten der Regel.
4. Aktivieren Sie die Option **Regel für zyklische Prüfung und Risikobewertung im IT Shop**.
5. Grenzen Sie die betroffenen Berechtigungen über die Option **mindestens eine Funktion** ein und wählen Sie die zu prüfenden SAP Funktionen.
    a. Wenn Sie mehr als eine SAP Funktion ausgewählt haben, legen Sie unter **Anzahl der zugewiesenen Berechtigungen** fest, wie viele SAP Funktionen

getroffen sein müssen, damit die Regel verletzt wird.

b. Führen SAP Berechtigungen erst in ihrer Kombination zu einer Regelverletzung, fügen Sie für jede betroffene SAP Funktion einen eigenen Regelblock ein.

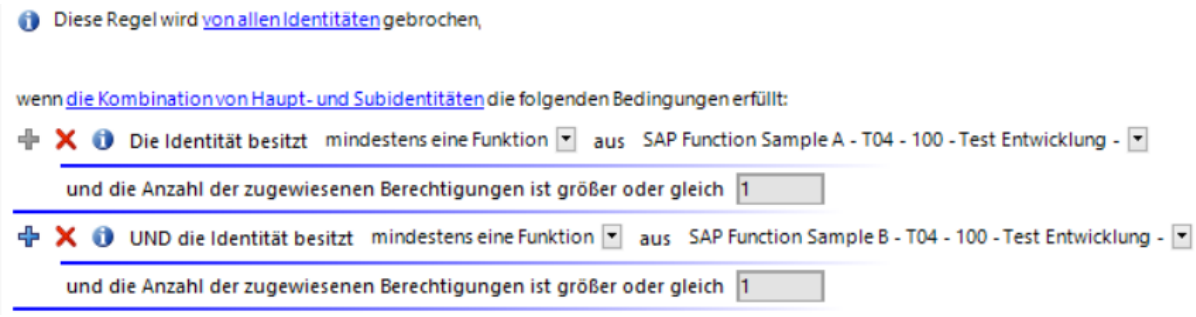
6. Speichern Sie die Änderungen.

   Es wird eine Arbeitskopie angelegt.

7. Wählen Sie die Aufgabe **Arbeitskopie aktivieren** und bestätigen Sie die Sicherheitsabfrage mit **OK**.

   Es wird eine aktive Regel in der Datenbank angelegt. Die Arbeitskopie bleibt bestehen und wird für nachfolgende Regeländerungen genutzt.

Abbildung 5: Bedingung für SAP Funktionen



Der One Identity Manager ermittelt bei der Regelprüfung alle Identitäten, die über die ihnen zugeordneten SAP Benutzerkonten die in der Regel angegebenen SAP Funktionen treffen. Ein SAP Benutzerkonto trifft eine SAP Funktion, wenn

- eine SAP Rolle, die dem SAP Benutzerkonto zugewiesen ist, die SAP Funktion trifft

  - ODER -

- eine SAP Rolle, die einem Referenzbenutzer zugewiesen ist, die SAP Funktion trifft

  - UND -

- dem SAP Benutzerkonto dieser Referenzbenutzer zugeordnet ist

Ausführliche Informationen zum Erstellen von Regelbedingungen finden Sie im *One Identity Manager Administrationshandbuch für Complianceregeln*.

Verwandte Themen

- Beispiele für SAP Funktionen auf Seite 30

Risikomindernde Maßnahmen für Complianceregeln mit SAP Funktionen

In Regeln über SAP Funktionen werden automatisch die risikomindernden Maßnahmen übernommen, die den zu prüfenden Funktionsdefinitionen zugewiesen sind. Die Bedingungen dafür sind:

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

Verwandte Themen

- Risikomindernde Maßnahmen an SAP Funktionen zuweisen auf Seite 46

Weitere Berichte über Regelverletzungen

One Identity Manager stellt verschiedene Berichte zur Verfügung, in denen Informationen über das ausgewählte Basisobjekt und seine Beziehungen zu anderen Objekten der One Identity Manager-Datenbank aufbereitet sind. Für aktive Complianceregeln für SAP Funktionen können zusätzliche Berichte erstellt werden.

Tabelle 18: Berichte über Regelverletzungen mit SAP Funktionen

Bericht	Beschreibung
Regelverletzungen mit SAP Appli-kationen	Der Bericht stellt alle Regelverletzungen für die ausgewählte Regel zusammen. Er liefert Ergebnisse für Regeln die SAP Funktionen prüfen. Zu jeder Identität werden alle Funktionsausprägungen mit ihren SAP Applikationen aufgelistet, durch welche die Identität die Regel verletzt. Zu jeder SAP Applikation werden die SAP Profile mit ihren Berechtigungsobjekten dargestellt, welche die SAP Funktion treffen.
Regelverletzungen mit SAP Rollen	Der Bericht stellt alle Regelverletzungen für die ausgewählte Regel zusammen. Er liefert Ergebnisse für Regeln die SAP Funktionen prüfen. Zu jeder Identität werden die SAP Gruppen, SAP Rollen und SAP Profile und deren Berechtigungsobjekte aufgelistet, durch die die Identität die Regel verletzt.

Bericht	Beschreibung
SAP Rollen und Profile mit Regel-verletzungen	Der Bericht zeigt alle SAP Rollen und Profile, die SAP Funktionen treffen und dadurch die ausgewählte Regel verletzen.

Risikomindernde Maßnahmen für SAP Funktionen

Für Unternehmen kann die Verletzung von regulatorischen Anforderungen unterschiedliche Risiken bergen. Um diese Risiken zu bewerten, können an SAP Funktionen Risikoindizes angegeben werden. Diese Risikoindizes geben darüber Auskunft, wie riskant eine Verletzung der jeweiligen SAP Funktion 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 SAP Funktion getroffen wurde. Nach Umsetzung der Maßnahmen sollte die nächste Berechnung keine unzulässigen Berechtigungen für diese SAP Funktion ermitteln.

Um risikomindernde Maßnahmen zu bearbeiten

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

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

Ausführliche Informationen über risikomindernde Maßnahmen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.

Detaillierte Informationen zum Thema

- Stammdaten für risikomindernde Maßnahmen erfassen auf Seite 61
- Überblick über eine risikomindernde Maßnahme auf Seite 61
- Funktionsdefinitionen an risikomindernde Maßnahmen zuweisen auf Seite 62
- Risikominderung für SAP Funktionen berechnen auf Seite 63

Stammdaten für risikomindernde Maßnahmen erfassen

Um risikomindernde Maßnahmen zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Risikoindex-Berechnungsvorschriften > Risikomindernde Maßnahmen**.
2. Wählen Sie in der Ergebnisliste eine risikomindernde Maßnahme und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Für eine risikomindernde Maßnahme erfassen Sie folgende Stammdaten.

Tabelle 19: 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.

Verwandte Themen

- Risikomindernde Maßnahmen für SAP Funktionen auf Seite 60

Überblick über eine 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**.
2. Öffnen Sie in der Navigationsansicht den Menüeintrag **Risikomindernde Maßnahme**.
3. Wählen Sie in der Ergebnisliste die risikomindernde Maßnahme.
4. Wählen Sie die Aufgabe **Überblick über die risikomindernde Maßnahme**.

Verwandte Themen

- Risikomindernde Maßnahmen für SAP Funktionen auf Seite 60

Funktionsdefinitionen an risikomindernde Maßnahmen zuweisen

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

Um SAP Funktionsdefinitionen an eine risikomindernde Maßnahme 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 **Funktionsdefinitionen zuweisen**.

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

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Risikomindernde Maßnahmen an SAP Funktionen zuweisen auf Seite 46
- Risikomindernde Maßnahmen für SAP Funktionen auf Seite 60

Risikominderung für SAP Funktionen berechnen

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

Verwandte Themen

- Risikomindernde Maßnahmen für SAP Funktionen auf Seite 60

Anhang A

Konfigurationsparameter für SAP Funktionen

Mit der Installation des Moduls sind zusätzlich folgende Konfigurationsparameter im One Identity Manager verfügbar.

Tabelle 20: Konfigurationsparameter für das Modul

Konfigurationsparameter	Beschreibung
TargetSystem | SAPR3 | SAPRights	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Überprüfung von Berechtigungen in einer SAP R/3-Umgebung durch SAP Funktionen. Ist der Parameter aktiviert, sind die Bestandteile des Moduls verfügbar. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
TargetSystem | SAPR3 | SAPRights | TestWithoutTCD	Prüfen der SAP Berechtigungen ohne Berücksichtigung der SAP Applikationen.

Die folgenden Konfigurationsparameter werden zusätzlich benötigt.

Tabelle 21: Zusätzliche Konfigurationsparameter

Konfigurationsparameter	Beschreibung
QER | CalculateRiskIndex	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Berechnung des Risikoindex. Nach Änderung des Parameters müssen Sie

Konfigurationsparameter	Beschreibung
	die Datenbank kompilieren. Ist der Parameter aktiviert, können Werte für den Risikoindex erfasst und berechnet werden. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
QER | ComplianceCheck	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Überprüfung des Regelwerkes. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Sie die Modellbestandteile nutzen. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.

Anhang B

Standardprojektvorlage für das Modul SAP R/3 Compliance Add-on

Eine Standardprojektvorlage sorgt dafür, dass alle benötigten Informationen im One Identity Manager angelegt werden. Dazu gehören beispielsweise die Mappings, Workflows und das Basisobjekt der Synchronisation. Wenn Sie keine Standardprojektvorlage verwenden, müssen Sie das Basisobjekt der Synchronisation selbst im One Identity Manager bekannt geben.

Verwenden Sie eine Standardprojektvorlage für die initiale Einrichtung des Synchronisationsprojektes. Für kundenspezifische Implementierungen können Sie das Synchronisationsprojekt mit dem Synchronization Editor erweitern.

Für die Synchronisation von Berechtigungsobjekten und Transaktionen nutzen Sie die Projektvorlage **SAP R/3 Berechtigungsobjekte**. Die Projektvorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 22: Abbildung der SAP R/3-Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im Zielsystem	Tabelle im One Identity Manager Schema
TOBJ	SAPAuthObject
ObjectClass	SAPAuthObjectClass
AUTHX	SAPField
Transaktionen	SAPTransaction
TACT	SAPActivity
ObjectHasField	SAPAuthObjectHasField
ObjectHasActivity	SAPAuthObjectHasSapActivity
FieldHasRcTable	SAPFieldHasSAPRCTable
TMENU01	SAPMenu
MenuHasTransaction	SAPMenuHasSAPTransaction

Schematyp im Zielsystem	Tabelle im One Identity Manager Schema
ProfileHasAuthObjectField	SAPProfileHasAuthObjectElem
RcTable	SAPRCTable
Variable	SAPRCVariable
TRANSACTIONHASTOBJ	SAPTransactionHasSAPAuthObject
RFCFUNCTION	SAPTransaction
USOBHASH	SAPTransaction

Anhang C

Referenzierte SAP R/3-Tabellen und BAPI-Aufrufe

Folgende Übersicht gibt Auskunft über alle während der Synchronisation von SAP Berechtigungsobjekten referenzierten Tabellen in einer SAP R/3-Umgebung und die ausgeführten BAPI-Aufrufe. Tabellen und BAPIs, auf die der SAP R/3 Konnektor bei der Synchronisation der SAP R/3 Basisadministration zugreift, sind im One Identity Manager Administrationshandbuch für die Anbindung einer SAP R/3-Umgebung aufgelistet.

Tabelle 23: Referenzierte Tabellen und BAPIs

Tabellen	BAPI-Aufrufe
AUTHX	/VIAENET/LISTMENU01
OBJCT	AUTH_TRACE_GET_USOBHASH
TACT	RFC_READ_TABLE
TACTZ	
TFDIR	
TMENU01	
TMENU01R	
TMENU01T	
TOBJ	
TOBCT	
TSTCT	
USOBHASH	
USOBX_C	
USR10	
UST10S	
UST12	
USVART	

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

Index

A

Anwendungsrolle
- Pflege SAP Funktionen 51

Arbeitskopie
- aktivieren 23
- Berechtigungsdefinition exportieren 38
- erstellen 37
- Funktionsdefinition exportieren 38
- risikomindernde Maßnahme zuweisen 46
- Überblicksformular 36

B

Benutzerkonto
- Referenzbenutzer 56

Berechtigung
- prüfen 5

Berechtigungsdefinition 17
- Bearbeitungsstatus 18
- Beispiel 30
- Berechtigungsfeld 18
- exportieren 37
- Variable 18, 43
- Variable in Variablenset übernehmen 45
- Wert 18

Berechtigungseditor 17-18

Berechtigungsobjekt 17-18

C

Complianceregel 5, 56

F

Feldvariable 43

Funktionsausprägung 13, 40
- Variablen prüfen 42

Funktionsdefinition 13
- Arbeitskopie 14, 35
- Auswirkung 15
- bearbeiten 35
- erstellen 14
- exportieren
  - alle 52
  - einzeln 37
- Gefährdungsgrad 15
- Verantwortliche 15

Funktionskategorie 48

I

Identity Audit 5

K

Konfigurationsparameter
- SAP Funktion 9

P

Plugin
SAP Funktion 52-53
Projektvorlage 66

R

Regelbedingung
Funktion 56
Regelverletzung
Beispiel 30
Risikobewertung
Unternehmensbereich 49
Risikoindex
berechnen 63
reduziert
berechnen 63
Risikomindernde Maßnahme
erfassen 61
erstellen 47
SAP Funktion 60
SAP Funktion zuweisen 47, 62
Signifikanzminderung 61
Überblick 61
zuweisen (SAP Funktionsdefinition) 47

S

SAP Funktion
Complianceregel 56
SAP Applikation 17-18
SAP Berechtigungsobjekte
Synchronisation
starten 10
Synchronisationsprojekt erstellen 10
SAP Berechtigungszuweisung
Probleme bei der Synchronisation 11
SAP Funktion 5
anwenden 30
Funktionsdefinition 15
importieren 53
Verantwortliche 40-41
SAP Funktionskategorie 48
Signifikanzminderung 61
Synchronisation
SAP Berechtigungsobjekte
konfigurieren 10-11
redundante Ausprägungen 11
Synchronisationsprojekt erstellen 10
Synchronisationsprojekt
Projektvorlage 66
Systemvariable 21

U

Überblicksformular
Funktionsausprägung 42
Funktionsdefinition 36
Unternehmensbereich 49

V

Variable 13
Systemvariable 21
Verwendung prüfen 42
Variablenname 21
Variablenset 43
kopieren 45

SAP Funktion 41
Überblicksformular 46
Variablen übernehmen 45