One Identity Manager 8.0.2

Administrationshandbuch für das SAP R/3 Compliance Add-on

Legende

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

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

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

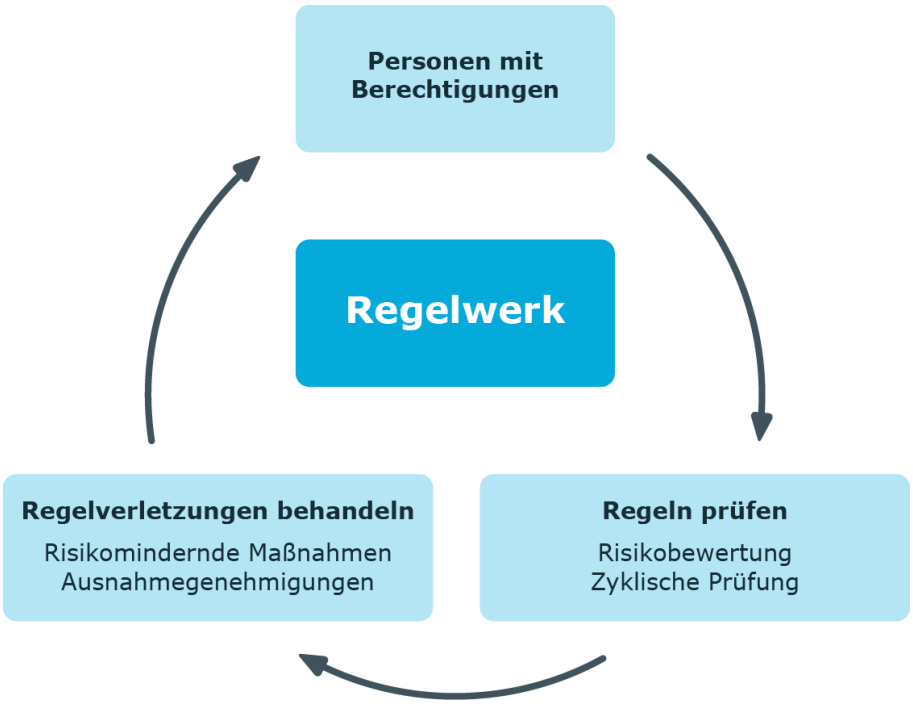
One Identity Manager Administrationshandbuch für das SAP R/3 Compliance Add-on
Aktualisiert - September 2018
Version - 8.0.2

Inhalt

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 Personen im Unternehmen überprüft werden sollen. Durch die Regelprüfung können einerseits bestehende Regelverletzungen gefunden werden. Andererseits können mögliche Regelverletzungen präventiv identifiziert und damit vermieden werden.

Abbildung 1: Identity Audit im One Identity Manager



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 Personen können auch Kombinationen von SAP Berechtigungen überprüft werden, die eine Person 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 Transaktionen und Berechtigungsobjekte überprüft. Dafür definieren Sie im One Identity Manager die zu prüfenden Transaktionen und zugehörigen Berechtigungsobjekte als sogenannte SAP Funktionen. Der One Identity Manager ermittelt alle SAP Rollen und Profile, denen genau diese Berechtigungsobjekte und Transaktionen 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 Personen diese SAP Funktionen treffen.

Erhalten Personen 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.

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 Regel-verantwortlichen zu. • Können bei Bedarf die Regelprüfung starten und Regel-

Benutzer	Aufgaben
	verletzungen 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 eine 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	• Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.
Compliance & Security Officer	Compliance & Security Officer müssen der Anwendungsrolle **Identity & Access Governance | Compliance & Security Officer**

Benutzer	Aufgaben
	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 und Risikoindex-Berechnungsvorschriften. • Können Attestierungsrichtlinien bearbeiten.

Voraussetzungen für die Einrichtung von SAP Funktionen

Tabelle 2: Konfigurationsparamter zur Bearbeitung von SAP Funktionen

Konfigurationsparameter	Bedeutung
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.
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.

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. Prüfen Sie im Designer, ob die Konfigurationsparameter "QER\ComplianceCheck" und "TargetSystem\SAPR3\SAPRights" aktiviert sind. Anderenfalls aktivieren Sie die Konfigurationsparameter und kompilieren Sie die Datenbank.
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

2

Erstellen eines Synchronisationsprojekts für die Synchronisation von SAP Berechtigungsobjekten

SAP Berechtigungen werden auf der Basis der für ein SAP Benutzerkonto zulässigen Transaktionen und Berechtigungsobjekte überprüft. Um SAP Funktionen erstellen zu können, müssen die Berechtigungsobjekte und Transaktionen 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.

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

Detaillierte Informationen zum Thema

- One Identity Manager Administrationshandbuch für die Anbindung einer SAP R/3-Umgebung
- One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation

Verwandte Themen

- Anhang: Standardprojektvorlage für das Modul SAP R/3 Compliance Add-on auf Seite 57
- Anhang: Referenzierte SAP R/3-Tabellen und BAPI-Aufrufe auf Seite 59

3

Basisdaten für SAP Funktionen

Für SAP Funktionen sind folgende Basisdaten relevant:

- Konfigurationsparameter

  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 Anhang: Konfigurationsparameter für SAP Funktionen auf Seite 56.

- SAP Funktionskategorien

  SAP Funktionskategorien verwenden Sie um SAP Funktionen nach spezifischen Kriterien zu gruppieren. Weitere Informationen finden Sie unter SAP Funktionskategorien auf Seite 13.

- 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. Weitere Informationen finden Sie unter Unternehmensbereiche auf Seite 13.

- Pflege SAP Funktionen

  An SAP Funktionen können Personen zugewiesen werden, die inhaltlich für diese SAP Funktionen verantwortlich sind und damit die Arbeitskopien bearbeiten können. Weitere Informationen finden Sie unter Pflege SAP Funktionen auf Seite 15.

SAP Funktionskategorien

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

Um eine Funktionskategorien zu bearbeiten

1. Wählen Sie die Kategorie **Identity Audit | Basisdaten zur Konfiguration | SAP Funktionskategorien**.
2. Wählen Sie in der Ergebnisliste eine Funktionskategorie. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - 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 3: Eigenschaften einer SAP Funktionskategorie

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

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.

Beispiel für den 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. Definieren Sie Bewertungskriterien für die Unternehmensbereiche.
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 bearbeiten

1. Wählen Sie die Kategorie **Identity Audit | Basisdaten zur Konfiguration | Unternehmensbereiche**.
2. Wählen Sie in der Ergebnisliste einen Unternehmensbereich. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - 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 4: 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 auf Seite 52

Pflege SAP Funktionen

An SAP Funktionen können Personen zugewiesen werden, die inhaltlich für diese SAP Funktionen verantwortlich sind. Im One Identity Manager ist eine Standardanwendungsrolle für die Pflege von SAP Funktionen vorhanden. Dieser Anwendungsrolle weisen Sie die Personen zu, die berechtigt sind, die Arbeitskopie dieser SAP Funktion zu bearbeiten, zu aktivieren und Funktionsausprägungen zu definieren. Bei Bedarf erstellen Sie weitere Anwendungsrollen. Ausführliche Informationen zum Einsatz und zur Bearbeitung von Anwendungsrollen finden Sie im One Identity Manager Administrationshandbuch für Anwendungsrollen.

Tabelle 5: 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 eine 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 Verantwortliche für die Pflege einer SAP Funktion festzulegen

1. Wählen Sie 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 in der Auswahlliste **Verantwortliche** die Anwendungsrolle.

   - ODER -

Klicken Sie neben der Auswahlliste **Verantwortliche** auf , um eine neue Anwendungsrolle zu erstellen.

- Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Identity & Access Governance | Identity Audit | Pflege SAP Funktionen** zu.
- Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.

5. Speichern Sie die Änderungen.
6. Weisen Sie der Anwendungsrolle die Personen zu, die berechtigt sind, die Funktionsdefinition zu bearbeiten.

Um Personen in eine Anwendungsrolle aufzunehmen

1. Wählen Sie in der Kategorie **Identity Audit | Basisdaten zur Konfiguration | Pflege SAP Funktionen** die Anwendungsrolle.
2. Wählen Sie die Aufgabe **Personen zuweisen**.
3. Weisen Sie die Personen zu und speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten einer Funktionsdefinition auf Seite 28

4

Ermitteln unzulässiger Berechtigungen

Tabelle 6: Konfigurationsparameter für die Berechtigungsprüfung

Konfigurationsparameter	Beschreibung
TargetSystem\SAPR3\SAPRights\TestWithoutTCD	Prüfen der SAP Berechtigungen ohne Berücksichtigung der SAP Transaktionen.

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

Bei der Berechtigungsprüfung wird der Konfigurationsparameter "TargetSystem\SAPR3\SAPRights\TestWithoutTCD" ausgewertet. Wenn der Konfigurationsparameter deaktiviert ist (Standardfall), gelten für die Berechtigungsprüfung die folgenden Regeln:

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

1. es mindestens eine der Transaktionen enthält, die in der SAP Funktion definiert sind,
2. es alle Berechtigungsobjekte dieser Transaktion besitzt,
3. es alle unterschiedlichen Funktionselemente eines Berechtigungsobjekts besitzt,
4. mindestens eine der Ausprägungen ein und desselben Funktionselements definiert ist.

Eine SAP Rolle trifft eine SAP Funktion, wenn das SAP Profil dieser SAP Rolle mindestens eine der Transaktionen enthält, die in der SAP Funktion definiert sind. Dabei muss das SAP Profil alle Berechtigungsobjekte dieser Transaktion besitzen. Ist für ein Berechtigungsobjekt ein Funktionselement mit einer Liste unterschiedlicher Ausprägungen

definiert, trifft das SAP Profil die SAP Funktion, wenn es mindestens eine dieser Ausprägungen besitzt.

Wenn der Konfigurationsparameter "TargetSystem\SAPR3\SAPRights\TestWithoutTCD" aktiviert ist, werden bei der Berechtigungsprüfung die Transaktionen nicht berücksichtigt. In diesem Fall gelten für die Berechtigungsprüfung folgende Regeln:

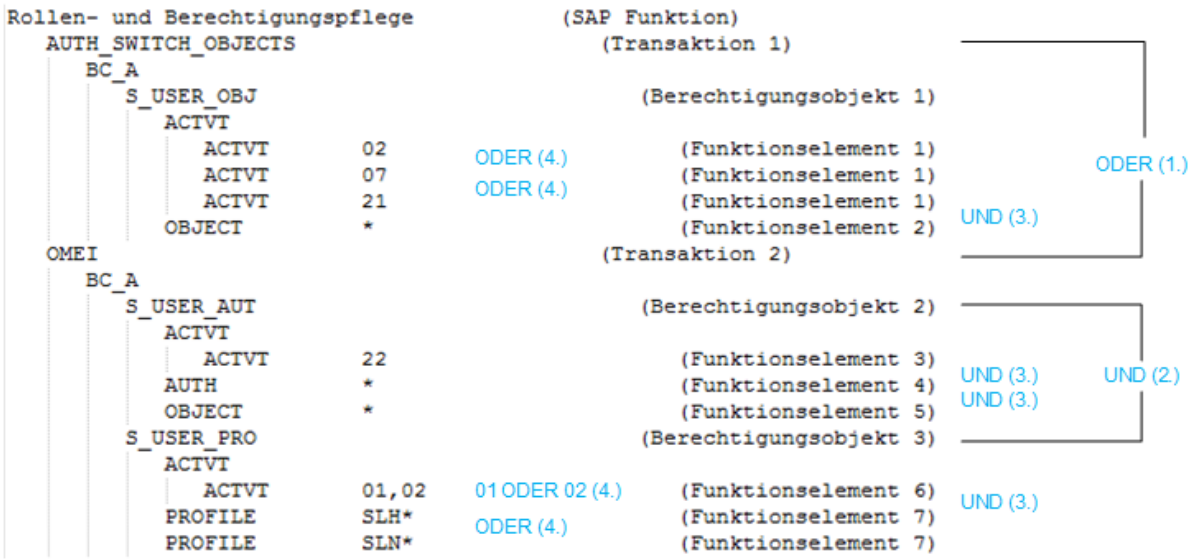
Eine SAP Rolle oder ein SAP Profil trifft eine SAP Funktion, wenn

1. es alle Berechtigungsobjekte aller Transaktionen besitzt,
2. es alle unterschiedlichen Funktionselemente eines Berechtigungsobjekts besitzt,
3. mindestens eine der Ausprägungen ein und desselben Funktionselements definiert ist.

Beispiel für eine Berechtigungsprüfung

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

Abbildung 2: Berechtigungsdefinition



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

- Transaktion 1 mit Berechtigungsobjekt 1 und Funktionselement 1 mit der Ausprägung "02" ODER "07" ODER "21" UND Funktionselement 2

  - ODER -

- Transaktion 2 mit Berechtigungsobjekt 2 und Funktionselement 3, 4 UND 5

  - UND -

  mit Berechtigungsobjekt 3 und Funktionselement 6 mit der Ausprägung "01" ODER "02" UND Funktionselement 7 mit der Ausprägung "SLH*" ODER "SLN*"

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

- Berechtigungsobjekt 1 und Funktionselement 1 mit der Ausprägung "02" ODER "07" ODER "21" UND Funktionselement 2

  - UND -

- Berechtigungsobjekt 2 und Funktionselement 3, 4 UND 5

  - UND -

- Berechtigungsobjekt 3 und Funktionselement 6 mit der Ausprägung "01" ODER "02" UND Funktionselement 7 mit der Ausprägung "SLH*" ODER "SLN*"

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 diese unzulässige Berechtigungskombination haben.

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

   Erstellen Sie SAP Funktionen für zulässige Berechtigungen oder Berechtigungskombination. Erstellen Sie Complianceregeln für SAP Funktionen, die sich gegenseitig ausschließen. Bei der Compliancеprüfung werden alle Personen gefunden, die über ihre 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 (SAP Rollen und Profile) 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 7: Beispiel für eine Berechtigungsdefinition

SAP Funktion	Transaktion	Berechtigungsobjekt	Feld	Wert
A	T1	BO2	ACTVT	*
	T1	BO2	CLASS	*
	T1	BO3	ACTVT	01, 02
	T2	BO5	ACTVT	*
	T2	BO5	CLASS	RST*
B	T1	BO3	ACTVT	*
	T1	BO4	ACTVT	02, 03, 07
	T1	BO4	CLASS	*

Folgende SAP Rollen sind vorhanden:

Tabelle 8: Definierte SAP Rollen

SAP Rolle	Transaktion	Berechtigungsobjekt	Feld	Wert
R1	T1	BO1	ACTVT	*
	T1	BO1	CLASS	*
	T1	BO3	ACTVT	*
	T1	BO4	ACTVT	01, 02
	T1	BO4	CLASS	DEF*
R2	T1	BO2	ACTVT	*
	T1	BO2	CLASS	*
	T1	BO3	ACTVT	*
R3	T1	BO4	ACTVT	03, 07
	T1	BO4	CLASS	*
R4	T2	BO5	ACTVT	03
	T2	BO5	CLASS	*

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

Tabelle 9: Ergebnisse der Berechtigungsprüfung

SAP Funktion	SAP Rolle	Konfigurationsparameter "TestWithoutTCD"	Begründung
B	R1	deaktiviert | aktiviert	Die Rolle R1 hat alle in der SAP Funktion benannten Berechtigungsobjekte und Felder sowie mindestens eine der Feldausprägungen. Der Rolle R2 fehlt das Berechtigungsobjekt BO4. Daher trifft sie die SAP Funktion nicht. Der Rolle R3 fehlt das Berechtigungsobjekt BO3. Daher trifft sie die SAP Funktion nicht. Der Rolle R4 fehlen die Berechtigungsobjekte BO3 und BO4. Daher trifft sie die SAP Funktion nicht. Da in der SAP Funktion nur eine Transaktion verwendet wird, hat der Konfigurationsparameter keine Auswirkung auf das Ergebnis der Berechtigungsprüfung.
A	R2, R4	deaktiviert	Die Rolle R2 hat alle in der Transaktion T1 benannten Berechtigungsobjekte, Felder und Ausprägungen. Die Rolle R4 hat alle in der Transaktion T2 benannten Berechtigungsobjekte, Felder und Ausprägungen. Der Rolle R1 fehlt das Berechtigungsobjekt BO2 oder BO5. Daher trifft sie die SAP Funktion nicht. Die Rolle R3 hat keine der benannten Berechtigungsobjekte. Daher trifft sie die SAP Funktion nicht.
A		aktiviert	Der Rolle R1 fehlen die Berechtigungsobjekte BO2 und BO5. Daher trifft sie die SAP Funktion nicht. Der Rolle R2 fehlt das Berechtigungsobjekt BO5. Daher trifft sie die SAP Funktion nicht. Die Rolle R3 hat keine der benannten Berechtigungsobjekte. Daher trifft sie die SAP Funktion nicht.

SAP Funktion	SAP Rolle	Konfigurationsparameter "TestWithoutTCD"	Begründung
			Der Rolle R4 fehlen die Berechtigungsobjekte BO2 und BO3. Daher trifft sie die SAP Funktion nicht.

Die SAP Rolle R3 entspricht den neuen Richtlinien und kann daher weiter genutzt werden. Die Rollen R1, R2 und R4 müssen den neuen Richtlinien angepasst werden. Wenn eine Berechtigungsprüfung ohne Berücksichtigung der Transaktionen zulässig ist, muss nur die Rolle R1 angepasst werden.

Beispiel für Anwendungsfall 2

Es soll nun geprüft werden, welche SAP Benutzerkonten den neuen Richtlinien widersprechen. Dafür müssen Complianceregeln für die SAP Funktionen erstellt werden.

Tabelle 10: Genutzte SAP Benutzerkonten

Personen	SAP Benutzerkonten	SAP Rollen	Berechtigungen
Clara Harris	K1	R1	BO1 | ACTVT {*}
			BO1 | CLASS {*}
			BO3 | ACTVT {*}
			BO4 | ACTVT {01, 02}
			BO4 | CLASS {DEF*}
Ben King	K2	R2, R3	BO2 | ACTVT {*}
			BO2 | CLASS {*}
			BO3 | ACTVT {*}
			BO4 | ACTVT {03, 07}
			BO4 | CLASS {*}
Jenny Basset	K3	R2	BO2 | ACTVT {*}
			BO2 | CLASS {*}
			BO3 | ACTVT {*}
Jenny Basset	K4	R3	BO4 | ACTVT {03, 07}
			BO4 | CLASS {*}
Jan Bloggs	K5	R3	BO4 | ACTVT {03, 07}
			BO4 | CLASS {*}

Dem Benutzerkonto K2 sind die SAP Rollen R2 und R3 zugewiesen. Damit erhält dieses Benutzerkonto alle Berechtigungen dieser beiden Rollen. Entsprechend der neuen Richtlinie darf eine Person jedoch nicht gleichzeitig die Berechtigungen BO3 und BO4 besitzen (SAP

Funktion B). Es wird daher eine Complianceregel erstellt, die alle Personen ermittelt, welche die SAP Funktion B treffen (Regel CR1). Da jedoch weder die Rolle R2 noch die Rolle R3 diese SAP Funktion trifft, wird keine Regelverletzung ermittelt.

Damit der One Identity Manager diese Regelverletzung erkennt, müssen für die Berechtigungsobjekte, die sich widersprechen, eigene SAP Funktionen erstellt werden. In einer Complianceregel werden daraufhin die SAP Funktionen kombiniert, die zu einer Regelverletzung führen.

Tabelle 11: Weitere SAP Funktionen

SAP Funktion	Transaktion	Berechtigungsobjekt	Feld	Wert
B	T1	BO3	ACTVT	*
	T1	BO4	ACTVT	02, 03, 07
	T1	BO4	CLASS	*
C	T1	BO3	ACTVT	*
D	T1	BO4	ACTVT	02, 03, 07
	T1	BO4	CLASS	*

Tabelle 12: Complianceregeln

Regel	Regelbedingung	Personen, welche die Regeln verletzen
CR1	Der Mitarbeiter besitzt die SAP Funktion B.	Clara Harris
CR2	Der Mitarbeiter besitzt die SAP Funktion C UND der Mitarbeiter besitzt die SAP Funktion D.	Clara Harris Ben King Jenny Basset

Jan Bloggs verletzt keine der Complianceregeln. Die SAP Rolle R3 trifft zwar die SAP Funktion D, diese führt aber nur in der Kombination mit der SAP Funktion C zu einer Regelverletzung.

Verwandte Themen

- Ermitteln unzulässiger Berechtigungen auf Seite 17
- Regelbedingungen für SAP Funktionen auf Seite 49

Hinweise für die Berechtigungsdefinition

Beim Erstellen einer Berechtigungsdefinition im Berechtigungseditor berücksichtigen Sie folgende Hinweise:

- Um zu einem Berechtigungsobjekt einen zusätzlichen Wert für das ACTVT-Element hinzuzufügen, klicken Sie **+**. Mehrere zulässige Werte von ACTVT-Elementen können auch als kommagetrennte Liste erfasst werden.
- Um zu einem Berechtigungsobjekt einen zusätzlichen Wert für ein anderes Funktionselement hinzuzufügen (beispielsweise CLASS), klicken Sie **C** neben diesem Funktionselement. Die zulässigen Werte dieser Funktionselemente können nicht als kommagetrennte Liste erfasst werden. Sie müssen immer als separate Einträge in der Berechtigungsdefinition erscheinen.
- Berechtigungsobjekte können innerhalb einer Berechtigungsdefinition nicht mehrfach eingefügt werden. Wenn eine Funktionsprüfung auf ein und dasselbe Berechtigungsobjekt mit unterschiedlichen Ausprägungen ausgeführt werden soll, erstellen sie für jede Ausprägung eine separate SAP Funktion. Kombinieren Sie diese SAP Funktionen in einer Complianceregel.

Detaillierte Informationen zum Thema

- Berechtigungseditor auf Seite 30
- Ermitteln unzulässiger Berechtigungen auf Seite 17

Verwandte Themen

- Beispiele für SAP Funktionen auf Seite 19
- Regelbedingungen für SAP Funktionen auf Seite 49

Einrichten von SAP Funktionen

Für SAP Funktionen erstellen Sie Funktionsdefinitionen, Funktionsausprägungen und Variablensets. Eine Funktionsdefinition enthält neben allgemeinen Stammdaten die Berechtigungsdefinition. Eine Berechtigungsdefinition besteht aus mindestens einer Transaktion. Zu jeder Transaktion 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 nutzen Sie in der Berechtigungsdefinition Variablen. Die konkreten Werte der Variablen werden in Variablensets zusammengestellt und in den Funktionsausprägungen angewendet.

Verwenden von Variablen

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

Tabelle 13: Festlegungen für Variablen

Eigenschaft	Festlegung
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.

<table>
<tr><th>Eigenschaft</th><th>Festlegung</th></tr>
<tr><td>Wert</td><td>
<table>
<tr><th>Syntax (Beispiel)</th><th>SAP Berechtigung wird geprüft auf</th><th>Beispiele für Feldwerte im SAP System</th></tr>
<tr><td>*</td><td>beliebige Werte</td><td>ab | 1234</td></tr>
<tr><td>beliebige Zeichenkette (ab)</td><td>exakt den angegebenen Wert</td><td>ab</td></tr>
<tr><td>[*]</td><td>den Wert *</td><td>*</td></tr>
<tr><td>Zeichenkette [*] (ab[*])</td><td>Werte, die mit der angegebenen Zeichenkette beginnen und mit * enden</td><td>ab*</td></tr>
<tr><td>Zeichenkette* (ab*)</td><td>Werte, die mit der angegebenen Zeichenkette beginnen und mit einer beliebigen Zeichenkette enden</td><td>ab* | abcd</td></tr>
<tr><td>Komma-getrennte Liste (ab, 1234, c*)</td><td>einen der in der Liste enthaltenen Werte</td><td>ab | 1234 | c* | cde</td></tr>
</table>
</td></tr>
</table>

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

- Berechtigungseditor auf Seite 30
- Stammdaten eines Variablensets auf Seite 43

Funktionsdefinitionen erstellen

Für jede Funktionsdefinition wird in der Datenbank eine Arbeitskopie angelegt. Um Funktionsdefinitionen zu erstellen und 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 neue Funktionsdefinition zu erstellen

1. Wählen Sie 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 **Arbeitskopie aktivieren**. 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.

Um eine bestehende Funktionsdefinition zu bearbeiten

1. Wählen Sie 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 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**. Bestätigen Sie die Sicherheitsabfrage mit **OK**.

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

Allgemeine Stammdaten einer Funktionsdefinition

Tabelle 14: Konfigurationsparameter für die Risikobewertung von SAP Funktionen

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

Für eine Funktionsdefinition erfassen Sie folgende Stammdaten.

Tabelle 15: 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. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter "QER\CalculateRiskIndex" aktiviert ist.
Risikoindex	Gibt den Risikoindex unter Berücksichtigung der zugewiesenen

Eigenschaft	Beschreibung
(reduziert)	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 (bzw. 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 (bzw. 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.

Detaillierte Informationen zum Thema

- SAP Funktionskategorien auf Seite 13
- Pflege SAP Funktionen auf Seite 15
- Risikomindernde Maßnahmen auf Seite 52
- One Identity Manager Administrationshandbuch für Risikobewertungen

Zusätzliche Aufgaben für Arbeitskopien

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können.

Überblick über die Funktionsdefinition

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

Um einen Überblick über eine Arbeitskopie zu erhalten

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

Berechtigungseditor

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

Um die Berechtigungsdefinition zusammenzustellen

1. Wählen Sie 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 vier Aufgaben.
    - **1. Hinzufügen durch Menüvorlage...**.

Tabelle 16: Eigenschaften einer Menüvorlage

Eigenschaft	Beschreibung
SAP Menü anzeigen	Menüeinträge aus dem SAP Menü der SAP GUI aus.
Alle anderen Menüs	Menüeinträge aus allen anderen SAP Menüs aus.
System	SAP System, aus dem der Menübaum angezeigt werden soll.
Menü	Menübaum zur Auswahl der Menüeinträge. Es werden alle Transaktionen und Berechtigungsobjekte geladen, die über die ausgewählten Menüeinträge aufgerufen werden können. Als zusätzliche Information werden im Menübaum die mit einem Menüeintrag verknüpften Transaktionscodes in Klammern angezeigt.

- ODER -

- **2. Hinzufügen durch Transaktion...**.

Tabelle 17: Eigenschaften einer Transaktion

Eigenschaft	Beschreibung
Filter	Filter für die Liste der zur Verfügung stehenden Transaktionen.
Transaktion	Transaktionen, deren Berechtigungsobjekte in den Berechtigungseditor geladen werden sollen. Es werden alle Berechtigungsobjekte eingefügt, die mit der ausgewählten Transaktion verknüpft sind.

- ODER -

- **3. Hinzufügen durch Berechtigungsobjekt...**.

Tabelle 18: Eigenschaften von Berechtigungsobjekten

Eigenschaft	Beschreibung
Filter	Filter für die Liste der zur Verfügung stehenden Berechtigungsobjekte.
Berechtigungsobjekt	Berechtigungsobjekte, die in den Berechtigungseditor geladen werden sollen. Es werden alle Transaktionen eingefügt, mit denen das ausgewählte Berechtigungsobjekt verknüpft ist.

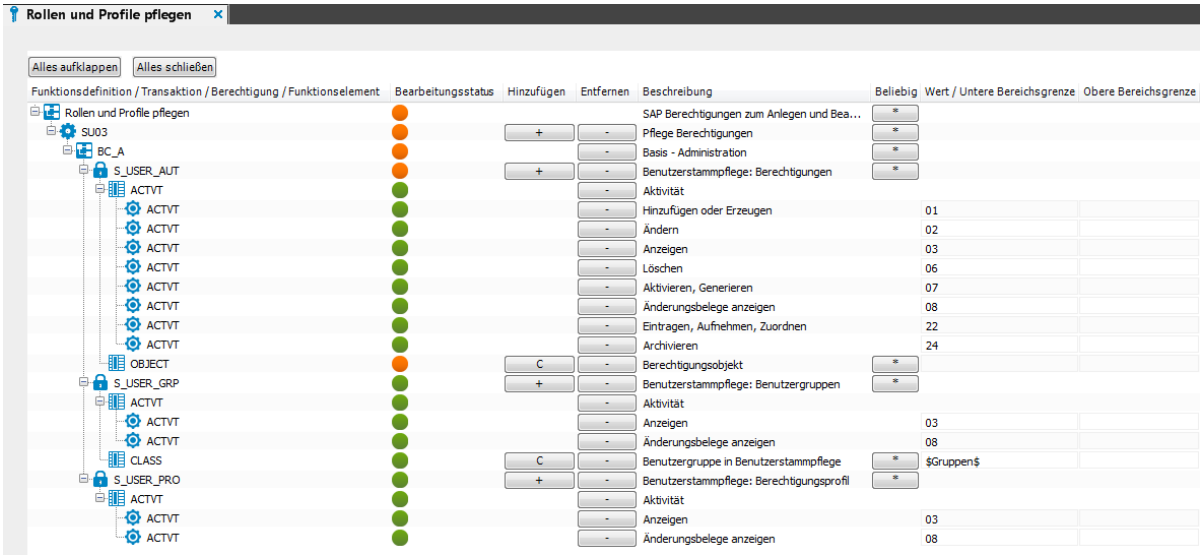
- ODER -

- **4. Hinzufügen durch vorhandene Funktionsdefinition...**.

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

5. Legen Sie die Details für die einzelnen Funktionselemente im Berechtigungseditor fest.
6. Speichern Sie die Änderungen.

Abbildung 3: Berechtigungseditor für SAP Funktionen



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

Tabelle 19: Eigenschaften einer Berechtigungsdefinition

Eigenschaft	Beschreibung
Funktionsdefinition / Transaktion / Berechtigung / Funktionselement	Hierarchie der Funktionsdefinition. Es werden Transaktionen, ihre zugehörigen Berechtigungsobjekte und Funktionselemente in einer Baumstruktur abgebildet.
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.

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td></td><td>Werte können als Variablen eingefügt werden. Es können auch Systemvariablen genutzt werden. In den Werten können Platzhalter genutzt werden.
<table>
<tr><th>Syntax (Beispiel)</th><th>SAP Berechtigung wird geprüft auf</th><th>Beispiele für Feldwerte im SAP System</th></tr>
<tr><td>*</td><td>beliebige Werte</td><td>ab | 1234</td></tr>
<tr><td>beliebige Zeichenkette (ab)</td><td>exakt den angegebenen Wert</td><td>ab</td></tr>
<tr><td>[*]</td><td>den Wert *</td><td>*</td></tr>
<tr><td>Zeichenkette [*] (ab[*])</td><td>Werte, die mit der angegebenen Zeichenkette beginnen und mit * enden</td><td>ab*</td></tr>
<tr><td>Zeichenkette* (ab*)</td><td>Werte, die mit der angegebenen Zeichenkette beginnen und mit einer beliebigen Zeichenkette enden</td><td>ab* | abcd</td></tr>
<tr><td>Komma-getrennte Liste (ab, 1234, c*)</td><td>einen der in der Liste enthaltenen Werte
Kommagetrennte Listen können nur an ACTVT-Elementen genutzt werden. An anderen Funktionselementen wird diese Liste wie eine Zeichenkette behandelt.</td><td>ab | 1234 | c* | cde</td></tr>
<tr><td>Variable (Var)</td><td>die in der Variable hinterlegten Werte</td><td></td></tr>
<tr><td>Systemvariable ($Var)</td><td>die in der Systemvariable hinterlegten Werte</td><td></td></tr>
</table>
</td></tr>
<tr><td>Obere Bereichs-grenze</td><td>Oberer Grenzwert für den Wertebereich eines Funktionselements. Werte können als Variablen eingefügt werden.</td></tr>
</table>

Innerhalb einer Transaktion 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 ein und desselben Funktionselements besitzt, definieren Sie diese Ausprägungen als kommagetrennte Werteliste für dieses Funktionselement.

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 20: 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

- Verwenden von Variablen auf Seite 25
- Variablensets anlegen auf Seite 42

Verwandte Themen

- Hinweise für die Berechtigungsdefinition auf Seite 24

Vollständigkeit der Berechtigungsobjekte prüfen

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

Um eine Berechtigungsdefinition auf Vollständigkeit zu prüfen

1. Wählen Sie 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. Schließen Sie das Fenster über die Schaltfläche **OK**.

   Die Berechtigungsobjekte können jetzt im Berechtigungseditor bearbeitet werden.

Berechtigungsübersicht

In der Berechtigungsübersicht werden die Funktionselemente in einer flachen Struktur dargestellt. Sie können hier alle Objekteigenschaften bearbeiten.

Um eine Übersicht aller Funktionselemente anzuzeigen

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

Arbeitskopie 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 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**.

Risikomindernde Maßnahmen

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 Regel 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 zuweisen auf Seite 36
- Risikomindernde Maßnahmen erstellen auf Seite 36
- Risikomindernde Maßnahmen auf Seite 52

Risikomindernde Maßnahmen zuweisen

Um risikomindernde Maßnahmen an eine Funktionsdefinition zuzuweisen

1. Wählen Sie 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**.
4. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die risikomindernden Maßnahmen, die zugewiesen werden sollen.

   – ODER –

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

Risikomindernde Maßnahmen erstellen

Um eine risikomindernde Maßnahme für SAP Funktionen zu erstellen

1. Wählen Sie 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 auf Seite 52

Arbeitskopie 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 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 21: Exportierte Stammdaten einer Funktionsdefinition

Eigenschaft	Datenfeld in der CSV-Datei
Name der Funktionsdefinition	Function
zugeordnete Funktionskategorie	Process
Beschreibung	Function Description
Auswirkung	Risk Level
Transaktionen	Transaction
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 47
- Funktionsdefinitionen exportieren auf Seite 46
- Funktionsdefinition exportieren auf Seite 39

Zusätzliche Aufgaben für Funktionsdefinitionen

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können.

Überblick über die Funktionsdefinition

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 die Kategorie **Identity Audit | SAP Funktionen | 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 anzuzeigen

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

Arbeitskopie erstellen

Um eine bestehende Funktionsdefinition zu ändern, bnötigen 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 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**.

Funktionsdefinition 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 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 22: Exportierte Stammdaten einer Funktionsdefinition

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

Eigenschaft	Datenfeld in der CSV-Datei
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 47
- Arbeitskopie exportieren auf Seite 37
- Funktionsdefinitionen exportieren auf Seite 46

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 Funktionsausprägungen zu bearbeiten

1. Wählen Sie die Kategorie **Identity Audit | SAP Funktionen | Funktionsausprägungen**.
2. Wählen Sie in der Ergebnisliste eine Funktionsausprägung. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Klicken Sie in der Ergebnisliste .
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.

Stammdaten einer Funktionsausprägung

Für Funktionsausprägungen erfassen Sie folgende Stammdaten.

Tabelle 23: 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 Transaktionen, 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 anlegen auf Seite 42
- Pflege SAP Funktionen auf Seite 15

Zusätzliche Aufgaben für Funktionsausprägungen

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können.

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

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 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**.

Variablensets anlegen

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

Um Variablensets zu bearbeiten

1. Wählen Sie die Kategorie **Identity Audit | SAP Funktionen | Variablensets**.
2. Wählen Sie in der Ergebnisliste ein Variablenset aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Stammdaten eines Variablensets

Für Variablensets erfassen Sie folgende Stammdaten.

Tabelle 24: 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 Feldvariablen zu bearbeiten

1. Um eine neue Zeile in die Liste einzufügen, klicken Sie **Hinzufügen**.

Tabelle 25: Eigenschaften einer Variable

Eigenschaft	Beschreibung
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.

2. Um die markierte Variable aus der Liste zu löschen, klicken Sie **Ausgewählte entfernen**.

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.

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 25

Zusätzliche Aufgaben für Variablensets

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können.

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

Variablenset kopieren

Um ein Variablenset zu kopieren

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 **Variablenset kopieren**.
5. Um die Stammdaten der Kopie sofort zu bearbeiten, klicken Sie **Ja**.
6. Bearbeiten Sie die Stammdaten der Kopie.
7. Speichern Sie die Änderungen.

Verwendete Variablen übernehmen

Variablen, die in 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 Variablen.
8. Speichern Sie die Änderungen.

Plugins für SAP Funktionen

Für SAP Funktionen stehen Ihnen zwei Plugins zur Verfügung. Die Plugins rufen Sie in der Menüleiste über das Menü **Plugins** auf. Über die Plugins können Sie in der One Identity Manager Datenbank vorhandene SAP Funktionen zwischen verschiedenen One Identity Manager Datenbanken austauschen.

Funktionsdefinitionen exportieren

Um alle Funktionsdefinitionen in eine CSV-Datei zu exportieren

1. Wählen Sie die Kategorie **Identity Audit**.
2. Wählen Sie das Menü **Plugins | Alle SAP Funktionsdefinitionen exportieren...**.
3. Klicken Sie **Ja**, um nur die Arbeitskopien zu exportieren.

   - ODER -

   Klicken Sie **Nein**, um nur die aktivierten SAP Funktionen zu exportieren.
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 26: Exportierte Stammdaten einer Funktionsdefinition

Eigenschaft	Datenfeld in der CSV-Datei
Name der Funktionsdefinition	Function
zugeordnete Funktionskategorie	Process
Beschreibung	Function Description
Auswirkung	Risk Level
Transaktionen	Transaction
Berechtigungsobjekte	Object
Berechtigungsfelder	Field
Beschreibung der Berechtigungsfelder	Field Description

Eigenschaft	Datenfeld in der CSV-Datei
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 47
- Arbeitskopie exportieren auf Seite 37
- Funktionsdefinition exportieren auf Seite 39

Funktionsdefinitionen importieren

Um SAP Funktionen aus einer vorhandenen CSV-Datei zu importieren, steht ebenfalls ein Plugin zur Verfügung. Die in der CSV-Datei enthaltenen Funktionsdefinitionen werden als Arbeitskopien in die Datenbank übertragen. Damit Funktionsdefinitionen importiert werden können, müssen folgende Datenfelder in der CSV-Datei vorhanden sein.

Tabelle 27: Datenfelder für den Import von Funktionsdefinitionen

Datenfeld in der CSV-Datei (Kopfzeile)	Objekteigenschaft im One Identity Manager
Pflichtfelder:	
Function	Funktionsdefinition
Transaction	Transaktion
Object	Berechtigungsobjekt
Field	Berechtigungsfeld
Value From	Wert/Untere Bereichsgrenze
Value To	Obere Bereichsgrenze
State	keine Entsprechung

Datenfeld in der CSV-Datei (Kopfzeile)	Objekteigenschaft im One Identity Manager
	Über den Importstatus wird geregelt, welche Datensätze in den One Identity Manager importiert werden sollen. 1 ... importieren
Optionale Felder:	
Process	Kategorie
Function Description	Beschreibung der Funktionsdefinition.
Risk Level	Auswirkung Mögliche Werte sind {Low|Medium|High|Critical}.
Field Description	Beschreibung der Berechtigungsfelder, Berechtigungsobjekte und Transaktionen.

HINWEIS: Die Reihenfolge der Datenfelder ist beliebig. Achten Sie darauf, dass alle benötigten Datenfelder in der Kopfzeile definiert und in den Datensätzen vorhanden sind. Datenfelder ohne Wert sind durch zwei aufeinanderfolgende Trennzeichen zu kennzeichnen. Datensätze mit fehlenden Pflichtfeldern werden nicht importiert.

Um Funktionsdefinitionen zu importieren

1. Wählen Sie die Kategorie **Identity Audit**.
2. Wählen Sie das Menü **Plugins | SAP Funktionsdefinitionen Import...**.
3. Wählen Sie die zu importierende CSV-Datei. 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.

Complianceregeln für SAP Funktionen

Neben den Berechtigungen, die eine Person 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 Rollenzuordnungen berücksichtigt.

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

Regelbedingungen für SAP Funktionen

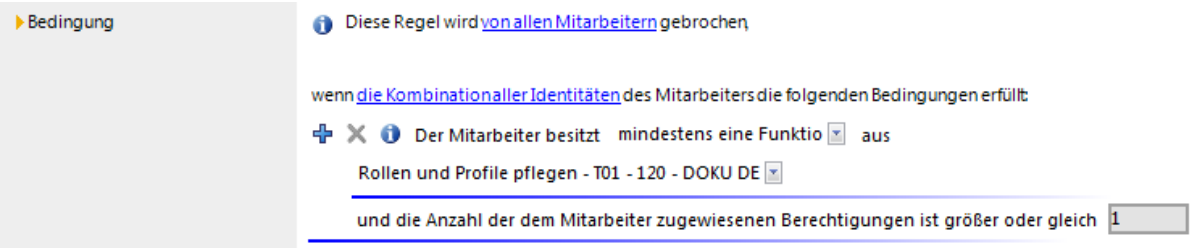
Um eine neue Regel für SAP Funktionen zu definieren

1. Wählen Sie 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 prüfende SAP Funktion.
   - 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**. 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 4: Bedingung für SAP Funktionen



Der One Identity Manager ermittelt bei der Regelprüfung alle Personen, 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

Detaillierte Informationen zum Thema

- One Identity Manager Administrationshandbuch für Complianceregeln

Weitere Berichte über Regelverletzungen

Tabelle 28: Berichte über Regelverletzungen

Bericht	Beschreibung
Regelverletzungen mit SAP Transaktionen	Der Bericht stellt alle Regelverletzungen für die ausgewählte Regel zusammen. Er liefert Ergebnisse für Regeln die SAP Funktionen prüfen. Zu jeder Person werden alle Funktionsausprägungen mit ihren Transaktionen aufgelistet, durch die die Person die Regel verletzt. Zu jeder Transaktion werden die SAP Profile mit ihren Berechtigungsobjekten dargestellt, die 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.

Bericht	Beschreibung
	Zu jeder Person werden die SAP Gruppen, SAP Rollen und SAP Profile und deren Berechtigungsobjekte aufgelistet, durch die die Person die Regel verletzt.

Risikomindernde Maßnahmen für Complianceregeln

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.

Risikomindernde Maßnahmen

Tabelle 29: Konfigurationsparameter für die Risikobewertung

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

Für Unternehmen kann die Verletzung von regulatorischen Anforderungen unterschiedliche Risiken bergen. Um diese Risiken zu bewerten, können an 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.

Detaillierte Informationen zum Thema

- One Identity Manager Administrationshandbuch für Risikobewertungen

Stammdaten erfassen

Um risikomindernde Maßnahmen zu bearbeiten

1. Wählen Sie die Kategorie **Risikoindex-Berechnungsvorschriften | Risikomindernde Maßnahmen**.
2. Wählen Sie in der Ergebnisliste eine risikomindernde Maßnahme. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   – 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 30: Allgemeine Stammdaten einer risikomindernden Maßnahme

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

Zusätzliche Aufgaben für risikomindernde Maßnahmen

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können.

Überblick über die risikomindernde Maßnahme

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

Um einen Überblick über eine risikomindernde Maßnahme zu erhalten

1. Wählen Sie 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**.

Funktionsdefinitionen 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 risikomindernde Maßnahmen zuzuweisen

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

   - ODER -

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

Risikominderung berechnen

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

Anhang: Konfigurationsparameter für SAP Funktionen

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

Tabelle 31: 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.
TargetSystem\SAPR3\SAPRights\TestWithoutTCD	Prüfen der SAP Berechtigungen ohne Berücksichtigung der SAP Trans-aktionen.

Anhang: 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 Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 32: 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
transaction	SAPTransaction
TACT	SAPActivity
objectHasField	SAPAuthObjectHasField
ObjectHasActivity	SAPAuthObjectHasSapActivity
FieldHasRcTable	SAPFieldHasSAPRCTable
tMenu01	SAPMenu

Schematyp im Zielsystem	Tabelle im One Identity Manager Schema
menuHasTransaction	SAPMenuHasSAPTransaction
ProfileHasAuthObjectField	SAPProfileHasAuthObjectElem
RcTable	SAPRCTable
RcVariable	SAPRCVariable
TRANSACTIONHASTOBJ	SAPTransactionHasSAPAuthObject

Anhang: 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 33: Referenzierte Tabellen und BAPIs

Tabellen	BAPI-Aufrufe
• AUTHX • DD04L • DD07L • TACT • TACTZ • TMENU01 • TMENU01R • TOBJ • TOBCT • TSTCT • USOBT_C • USR10 • UST10S • UST12 • USVART	• RFC_READ_TABLE

Über uns

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

Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen besuchen Sie https://www.oneidentity.com/company/contact-us.aspx oder rufen Sie + 1-800-306-9329 an.

Technische Supportressourcen

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

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

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

Index

S

T

U

V