One Identity Manager 9.1.3

Administrationshandbuch für Privileged Account Governance

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 Privileged Account Governance
Aktualisiert - 29. April 2024, 13:52 Uhr

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

Inhalt

Über dieses Handbuch ... **9**

Verwalten eines Privileged Account Management Systems im One Identity Manager ... **10**

Architekturüberblick ... 11

One Identity Manager Benutzer für die Verwaltung eines Privileged Account Management Systems ... 11

Konfigurationsparameter für die Verwaltung von Privileged Account Management Systemen ... 14

Synchronisieren eines Privileged Account Management Systems ... **15**

Einrichten der Initialsynchronisation mit One Identity Safeguard ... 16

Benutzer und Berechtigungen für die Synchronisation mit einer One Identity Safeguard Appliance ... 17

Einrichten des One Identity Safeguard Synchronisationsservers ... 19

Systemanforderungen für den One Identity Safeguard Synchronisationsserver ... 19

Windows PowerShell Modul safeguard-ps installieren ... 20

One Identity Manager Service mit One Identity Safeguard Konnektor installieren ... 20

Vorbereiten der administrativen Arbeitsstation für den Zugriff auf die One Identity Safeguard Appliance ... 24

Vorbereiten eines Remoteverbindungsservers für den Zugriff auf die One Identity Safeguard Appliance ... 25

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer One Identity Safeguard Appliance ... 26

Benötigte Informationen für die Erstellung eines Synchronisationsprojektes ... 26

Initiales Synchronisationsprojekt für One Identity Safeguard erstellen ... 28

Synchronisationsprotokoll konfigurieren ... 32

Anpassen der Synchronisationskonfiguration für One Identity Safeguard ... 33

Synchronisation in eine One Identity Safeguard Appliance konfigurieren ... 34

Synchronisation verschiedener One Identity Safeguard Appliances konfigurieren ... 35

Einstellungen der Systemverbindung zur One Identity Safeguard Appliance ändern ... 35

Verbindungsparameter im Variablenset bearbeiten ... 36

Eigenschaften der Zielsystemverbindung bearbeiten ... 37

Anpassen der Windows PowerShell Definition des One Identity Safeguard Konnektors ... 38

Schema aktualisieren ... 39
Beschleunigung der Synchronisation durch Revisionsfilterung ... 40
Provisionierung von Mitgliedschaften konfigurieren ... 40
Einzelobjektsynchronisation konfigurieren ... 42
Beschleunigung der Provisionierung und Einzelobjektsynchronisation ... 43
Ausführen einer Synchronisation ... 44
Synchronisationen starten ... 45
Synchronisationsergebnisse anzeigen ... 46
Synchronisation deaktivieren ... 47
Einzelobjekte synchronisieren ... 47
Aufgaben nach einer Synchronisation ... 48
Ausstehende Objekte nachbearbeiten ... 49
Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen ... 51
PAM Benutzerkonten über Kontendefinitionen verwalten ... 51
Fehleranalyse ... 52
Datenfehler bei der Synchronisation ignorieren ... 52
Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) ... 53

Managen von PAM Benutzerkonten und Personen ... 56
Kontendefinitionen für PAM Benutzerkonten ... 57
Kontendefinitionen erstellen ... 58
Kontendefinitionen bearbeiten ... 59
Stammdaten von Kontendefinitionen ... 59
Automatisierungsgrade bearbeiten ... 62
Automatisierungsgrade erstellen ... 63
Automatisierungsgrade an Kontendefinitionen zuweisen ... 64
Stammdaten von Automatisierungsgraden ... 64
Abbildungsvorschriften für IT Betriebsdaten erstellen ... 65
IT Betriebsdaten erfassen ... 67
IT Betriebsdaten ändern ... 68
Zuweisen der Kontendefinitionen an Personen ... 69
Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen ... 71
Kontendefinitionen an Geschäftsrollen zuweisen ... 71
Kontendefinitionen an alle Personen zuweisen ... 72
Kontendefinitionen direkt an Personen zuweisen ... 72
Kontendefinitionen an Systemrollen zuweisen ... 73

Kontendefinitionen in den IT Shop aufnehmen ... 73
Kontendefinitionen an PAM Appliances zuweisen ... 75
Kontendefinitionen löschen ... 76
Automatische Zuordnung von Personen zu PAM Benutzerkonten ... 79
Suchkriterien für die automatische Personenzuordnung bearbeiten ... 81
Personen suchen und direkt an Benutzerkonten zuordnen ... 82
Automatisierungsgrade für PAM Benutzerkonten ändern ... 84
Kontendefinitionen an verbundene PAM Benutzerkonten zuweisen ... 84
Personen manuell mit PAM Benutzerkonten verbinden ... 85
Unterstützte Typen von Benutzerkonten ... 86
Standardbenutzerkonten ... 87
Administrative Benutzerkonten ... 88
Administrative Benutzerkonten für eine Person bereitstellen ... 89
Administrative Benutzerkonten für mehrere Personen bereitstellen ... 90
Privilegierte Benutzerkonten ... 91
Löschverzögerung für PAM Benutzerkonten festlegen ... 92

Managen von Zuweisungen von PAM Benutzergruppen ... 94

Zuweisen von PAM Benutzergruppen an PAM Benutzerkonten im One Identity Manager ... 94
Voraussetzungen für indirekte Zuweisungen von PAM Gruppen an PAM Benutzerkonten ... 96
PAM Benutzergruppen an Abteilungen, Kostenstellen und Standorte zuweisen ... 97
PAM Benutzergruppen an Geschäftsrollen zuweisen ... 98
PAM Benutzergruppen in Systemrollen aufnehmen ... 99
PAM Benutzergruppen in den IT Shop aufnehmen ... 100
Lokale PAM Benutzergruppen automatisch in den IT Shop aufnehmen ... 102
PAM Benutzerkonten direkt an eine PAM Benutzergruppe zuweisen ... 104
PAM Benutzergruppen direkt an ein PAM Benutzerkonto zuweisen ... 104
Wirksamkeit von Mitgliedschaften in PAM Benutzergruppen ... 105
Vererbung von PAM Benutzergruppen anhand von Kategorien ... 108
Übersicht aller Zuweisungen ... 110

Bereitstellen von Anmeldeinformationen für PAM Benutzerkonten ... 112

Kennwortrichtlinien für PAM Benutzer ... 112
Vordefinierte Kennwortrichtlinien ... 113
Kennwortrichtlinien anwenden ... 114

Kennwortrichtlinien bearbeiten ... 116
Kennwortrichtlinien erstellen ... 116
Allgemeine Stammdaten für Kennwortrichtlinien ... 117
Richtlinieneinstellungen ... 117
Zeichenklassen für Kennwörter ... 119
Kundenspezifische Skripte für Kennwortanforderungen ... 120
Skript zum Prüfen eines Kennwortes ... 120
Skript zum Generieren eines Kennwortes ... 122
Ausschlussliste für Kennwörter bearbeiten ... 123
Kennwörter prüfen ... 123
Generieren von Kennwörtern testen ... 124
Initiales Kennwort für neue PAM Benutzerkonten ... 124
E-Mail-Benachrichtigungen über Anmeldeinformationen ... 125

Abbildung von PAM Objekten im One Identity Manager ... 127
PAM Appliances ... 127
PAM Appliances erstellen ... 128
Stammdaten von PAM Appliances bearbeiten ... 129
Allgemeine Stammdaten von PAM Appliances ... 129
Kategorien für die Vererbung von PAM Benutzergruppen definieren ... 131
Synchronisationsprojekt für eine PAM Appliance bearbeiten ... 132
Überblick über PAM Appliances anzeigen ... 132
PAM Benutzerkonten ... 132
Lokale PAM Benutzerkonten erstellen ... 134
Zertifikatsbasierte PAM Benutzerkonten erstellen ... 134
PAM Benutzerkonten für Verzeichnisbenutzer erstellen ... 135
Stammdaten für PAM Benutzerkonten bearbeiten ... 137
Allgemeine Stammdaten für PAM Benutzerkonten ... 138
Kontaktinformationen für PAM Benutzerkonten ... 143
Sekundäre Authentifizierung für PAM Benutzerkonten ... 144
Administrative Berechtigungen für PAM Benutzerkonten ... 145
Zusatzeigenschaften an PAM Benutzerkonten zuweisen ... 146
PAM Benutzerkonten deaktivieren ... 147
PAM Benutzerkonten löschen und wiederherstellen ... 148
Überblick über PAM Benutzerkonten anzeigen ... 149
PAM Benutzergruppen ... 149

Stammdaten für PAM Benutzergruppen bearbeiten ... 150
Allgemeine Stammdaten für PAM Benutzergruppen ... 150
Administrative Berechtigungen für PAM Benutzergruppen ... 152
Zusatzeigenschaften an PAM Benutzergruppen zuweisen ... 153
Überblick über PAM Benutzergruppen anzeigen ... 154
PAM Assets ... 154
PAM Assetgruppen ... 155
PAM Assetkonten ... 155
PAM Verzeichniskonten ... 156
PAM Kontogruppen ... 157
PAM Verzeichnisse ... 158
PAM Nutzungsrechte ... 159
PAM Zugriffsanforderungsrichtlinien ... 160
Berichte über PAM Objekte ... 160

PAM Zugriffsanforderungen ... 164
Systemanforderungen für die Bestellung von PAM Zugriffsanforderungen ... 165
Bestellen von PAM Zugriffsanforderungen ... 166
Eigentümer von PAM Objekten ... 167
Automatische Ermittlung der Eigentümer ... 168
Personen manuell als Eigentümer von PAM Objekten festlegen ... 169
Anwendungsrollen für Eigentümer von PAM Objekten manuell festlegen ... 170
Konfigurieren der PAM Zugriffsanforderungsrichtlinien ... 171

Behandeln von PAM Objekten im Web Portal ... 172

Basisdaten für die Verwaltung eines Privileged Account Management Systems ... 174
Zielsystemverantwortliche für PAM Systeme ... 175
Jobserver für PAM-spezifische Prozessverarbeitung ... 178
PAM Jobserver bearbeiten ... 178
Allgemeine Stammdaten für Jobserver ... 179
Festlegen der Serverfunktionen ... 182

Anhang: Konfigurationsparameter für die Verwaltung eines Privileged Account Management Systems ... 184

Anhang: Standardprojektvorlage für One Identity Safeguard ... 187

Anhang: Verarbeitung von One Identity Safeguard Systemobjekten ... 189

Anhang: Einstellungen des One Identity Safeguard Konnektors 190

Anhang: Bekannte Probleme bei der Anbindung einer One Identity Safeguard Appliance 192

Über uns 194

Kontaktieren Sie uns 194

Technische Supportressourcen 194

Index 195

Über dieses Handbuch

Das *One Identity Manager Administrationshandbuch für die Privileged Account Governance* beschreibt, wie Sie die Synchronisation von One Identity Safeguard mit dem One Identity Manager einrichten. Sie erfahren, wie im One Identity Manager die Benutzerkonten, Benutzergruppen, Assets, Assetgruppen, Konten, Kontogruppen, Verzeichnisse, Nutzungsrechte und Zugriffsanforderungsrichtlinien eines Privileged Account Management Systems verwaltet werden.

Dieses Handbuch wurde als Nachschlagewerk für End-Anwender, Systemadministratoren, Berater, Analysten und andere IT-Fachleute entwickelt.

HINWEIS: Dieses Handbuch beschreibt die Funktionen des One Identity Manager, die für den Standardbenutzer verfügbar sind. Abhängig von der Systemkonfiguration und den Berechtigungen stehen Ihnen eventuell nicht alle Funktionen zur Verfügung.

Verfügbare Dokumentation

Die One Identity Manager Dokumentation erreichen Sie im Manager und im Designer über das Menü **Hilfe** > **Suchen**. Die Online Version der One Identity Manager Dokumentation finden Sie im Support-Portal unter Online-Dokumentation. Videos mit zusätzlichen Informationen finden Sie unter www.YouTube.com/OneIdentity.

2

Verwalten eines Privileged Account Management Systems im One Identity Manager

Der One Identity Manager bietet eine vereinfachte Administration der Benutzerkonten eines Privileged Account Management Systems. Dabei konzentriert sich der One Identity Manager auf die Einrichtung und Bearbeitung von Benutzerkonten und die Zuweisung der Benutzerkonten zu Benutzergruppen. Über die Benutzergruppen erhalten Benutzerkonten die Nutzungsrechte, um beispielsweise ein Kennwort für einen Assetkonto oder eine Sitzung für die Konten und Assets im Privileged Account Management System anfordern zu können. Die Zuweisung der Nutzungsrechte an die Benutzergruppen erfolgt nicht im One Identity Manager, sondern im Privileged Account Management System. Über das Web Portal können Benutzergruppen und Anforderungen für Kennwörter und Sitzungen bestellt werden.

Im One Identity Manager werden die Personen eines Unternehmens mit den benötigten Benutzerkonten versorgt. Dabei können Sie unterschiedliche Mechanismen für die Verbindung der Personen mit ihren Benutzerkonten nutzen. Ebenso können Sie die Benutzerkonten getrennt von Personen verwalten und somit administrative Benutzerkonten einrichten.

Im One Identity Manager werden die Benutzerkonten, Benutzergruppen, Assets, Assetgruppen, Konten, Kontogruppen, Verzeichnisse, Nutzungsrechte und Zugriffsanforderungsrichtlinien eines Privileged Account Management Systems abgebildet. Diese Objekte werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Damit ist es möglich, die Identity und Access Governance Prozesse wie Attestierung, Identity Audit, Management von Benutzerkonten und Systemberechtigungen, IT Shop oder Berichtsabonnements für Privileged Account Management Systeme zu nutzen.

HINWEIS: Voraussetzung für die Verwaltung eines Privileged Account Management Systems im One Identity Manager ist die Installation des Privileged Account Governance Moduls. Ausführliche Informationen zur Installation finden Sie im *One Identity Manager Installationshandbuch.*

Architekturüberblick

Um auf die Daten eines Privileged Account Management Systems zuzugreifen, wird auf einem Synchronisationsserver ein Konnektor für das Privileged Account Management System installiert. Der Synchronisationsserver sorgt für den Abgleich der Daten zwischen der One Identity Manager-Datenbank und dem Privileged Account Management System.

Der One Identity Manager unterstützt die Synchronisation mit One Identity Safeguard. Der One Identity Safeguard Konnektor des One Identity Manager verwendet Windows PowerShell für die Kommunikation mit der One Identity Safeguard Appliance.

One Identity Manager Benutzer für die Verwaltung eines Privileged Account Management Systems

In die Einrichtung und Verwaltung eines Privileged Account Management Systems sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Zielsystemadministratoren	Die Zielsystemadministratoren müssen der Anwendungsrolle **Zielsysteme | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen. • Legen die Zielsystemverantwortlichen fest. • Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein. • Legen fest, welche Anwendungsrollen für Zielsystemverantwortliche sich ausschließen. • Berechtigen weitere Personen als Zielsystemadministratoren. • Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Privileged Account Management** oder einer untergeordneten

Benutzer	Aufgaben
	Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen. • Berechtigen innerhalb ihres Verantwortungsbereiches Personen als Eigentümer von privilegierten Objekten.
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 Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse.

Benutzer	Aufgaben
	• Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.
Produkteigner für den IT Shop	Die Produkteigner müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Entscheiden über Bestellungen. • Bearbeiten die Leistungspositionen und Servicekategorien, für die sie verantwortlich sind. Bei der automatischen Übernahme von lokalen PAM Benutzergruppen in den IT Shop wird die Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner | PAM Benutzergruppen** verwendet.
Eigentümer privilegierter Objekte	Die Eigentümer privilegierter Objekte wie PAM Assets, PAM Assetkonten, PAM Verzeichniskonten, PAM Assetgruppen und PAM Kontogruppen müssen einer Anwendungsrolle unter der Anwendungsrolle **Privileged Account Governance | Asset- und Konteneigentümer** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Entscheiden über die Bestellung von Zugriffsanforderungen für privilegierte Objekte. • Attestieren den möglichen Zugriff von Benutzern auf diese privilegierten Objekte.
Administratoren für den IT Shop	Die Administratoren müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an IT Shop-Strukturen zu.
Administratoren für Organisationen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Organisationen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an Abteilungen, Kostenstellen und Standorte zu.
Administratoren für	Die Administratoren müssen der Anwendungsrolle

Benutzer	Aufgaben
Geschäftsrollen	**Identity Management | Geschäftsrollen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an Geschäftsrollen zu.

Konfigurationsparameter für die Verwaltung von Privileged Account Management Systemen

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 die Verwaltung eines Privileged Account Management Systems auf Seite 184.

3

Synchronisieren eines Privileged Account Management Systems

Der One Identity Manager unterstützt die Synchronisation mit One Identity Safeguard ab der Version 6.0. Für die im einzelnen unterstützten Versionen finden Sie auf dem One Identity Manager Installationsmedium im Verzeichnis `Modules\PAG\dvd\AddOn\safeguard-ps` das passende Windows PowerShell Modul. Versionen, für die kein Windows PowerShell Modul auf dem One Identity Manager Installationsmedium vorhanden ist, werden nicht unterstützt.

Für den Abgleich der Informationen zwischen der One Identity Manager-Datenbank und der One Identity Safeguard Appliance sorgt der One Identity Manager Service.

Informieren Sie sich hier:

- wie Sie die Synchronisation einrichten, um initial Daten aus einer One Identity Safeguard Appliance in die One Identity Manager-Datenbank einzulesen,
- wie Sie eine Synchronisationskonfiguration anpassen, beispielsweise um verschiedene One Identity Safeguard Appliances mit ein und demselben Synchronisationsprojekt zu synchronisieren,
- wie Sie die Synchronisation starten und deaktivieren,
- wie Sie die Synchronisationsergebnisse auswerten.

TIPP: Bevor Sie die Synchronisation mit einer One Identity Safeguard Appliance einrichten, machen Sie sich mit dem Synchronization Editor vertraut. Ausführliche Informationen über dieses Werkzeug finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Detaillierte Informationen zum Thema

- Einrichten der Initialsynchronisation mit One Identity Safeguard auf Seite 16
- Anpassen der Synchronisationskonfiguration für One Identity Safeguard auf Seite 33
- Ausführen einer Synchronisation auf Seite 44
- Aufgaben nach einer Synchronisation auf Seite 48
- Fehleranalyse auf Seite 52
- Datenfehler bei der Synchronisation ignorieren auf Seite 52

- Verarbeitung von One Identity Safeguard Systemobjekten auf Seite 189
- Bekannte Probleme bei der Anbindung einer One Identity Safeguard Appliance auf Seite 192

Einrichten der Initialsynchronisation mit One Identity Safeguard

Der Synchronization Editor stellt Projektvorlagen bereit, mit der die Synchronisation von Benutzerkonten und Berechtigungen einer Zielsystemumgebung eingerichtet werden kann. Zusätzlich werden die notwendigen Prozesse angelegt, über die Änderungen an Zielsystemobjekten aus der One Identity Manager-Datenbank in das Zielsystem provisioniert werden.

Nutzen Sie die Projektvorlage **One Identity Safeguard Synchronisation**, um Synchronisationsprojekte zu erstellen, mit denen Sie Daten aus einer One Identity Safeguard Appliance in Ihre One Identity Manager-Datenbank einlesen.

Um die Objekte initial in die One Identity Manager-Datenbank einzulesen

1. Stellen Sie im Privileged Account Management System einen Benutzer für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Die One Identity Manager Bestandteile für die Verwaltung von Privileged Account Management Systemen sind verfügbar, wenn der Konfigurationsparameter **TargetSystem | PAG** aktiviert ist.
    - Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.

      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*.
    - Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.
3. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
4. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Detaillierte Informationen zum Thema

- Benutzer und Berechtigungen für die Synchronisation mit einer One Identity Safeguard Appliance auf Seite 17
- Einrichten des One Identity Safeguard Synchronisationsservers auf Seite 19
- Vorbereiten der administrativen Arbeitsstation für den Zugriff auf die One Identity Safeguard Appliance auf Seite 24
- Vorbereiten eines Remoteverbindungsservers für den Zugriff auf die One Identity Safeguard Appliance auf Seite 25
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer One Identity Safeguard Appliance auf Seite 26
- Konfigurationsparameter für die Verwaltung eines Privileged Account Management Systems auf Seite 184
- Standardprojektvorlage für One Identity Safeguard auf Seite 187

Benutzer und Berechtigungen für die Synchronisation mit einer One Identity Safeguard Appliance

Bei der Synchronisation des One Identity Manager mit einer One Identity Safeguard Appliance spielen folgende Benutzer eine Rolle.

Tabelle 2: Benutzer für die Synchronisation

Benutzer	Berechtigungen

Benutzer für den Zugriff auf die One Identity Safeguard Appliance (Synchronisationsbenutzer)	Für eine vollständige Synchronisation von Objekten einer One Identity Safeguard Appliance mit der ausgelieferten One Identity Manager Standardkonfiguration stellen Sie auf der Appliance einen Benutzer mit folgenden Einstellungen bereit:
	• Authentifizierungsanbieter **Certificate**
	• Fingerabdruck eines Zertifikats, das auf der Appliance als vertrauenswürdiges Zertifikat hinterlegt ist
	• Berechtigungen:
	  • Autorisier
	  • Benutzer
	  • Help Desk
	  • Appliance

Benutzer	Berechtigungen
	• Vorgänge • Asset • Verzeichnis • Sicherheitsrichtlinie Ausführliche Informationen zu Benutzern und Zertifikaten im One Identity Safeguard finden Sie im *One Identity Safeguard Adminstration Guide*.
Benutzerkonto des One Identity Manager Service	Das Benutzerkonto für den One Identity Manager Service benötigt die Benutzerrechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Verzeichnisse und Dateien anlegen und bearbeiten. Das Benutzerkonto muss der Gruppe **Domänen-Benutzer** angehören. Das Benutzerkonto benötigt das erweiterte Benutzerrecht **Anmelden als Dienst**. Das Benutzerkonto benötigt Berechtigungen für den internen Webservice. HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so können Sie die Berechtigungen für den internen Webservice über folgenden Kommandozeilenaufruf vergeben: `netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"` Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis. In der Standardinstallation wird der One Identity Manager installiert unter: • `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen) • `%ProgramFiles%\One Identity` (auf 64-Bit Betriebssystemen) Das Benutzerkonto benötigt im Zertifikatsspeicher des aktuellen Benutzers das Zertifikat mit dem privaten Schlüssel, das auf der One Identity Safeguard Appliance als vertrauenswürdiges Zertifikat hinterlegt ist. Das Zertifikat muss dasselbe Zertifikat sein, welches auch der

Benutzer	Berechtigungen
	Synchronisationsbenutzer verwendet. Ausführliche Informationen zu Zertifikaten im One Identity Safeguard finden Sie im *One Identity Safeguard Adminstration Guide*. HINWEIS: Der Zugriff über das lokale Systemkonto **NT AUTHORITY\SYSTEM** wird nicht unterstützt.
Benutzer für den Zugriff auf die One Identity Manager-Datenbank	Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer **Synchronization** bereitgestellt.

Einrichten des One Identity Safeguard Synchronisationsservers

Vom Synchronisationsserver werden alle Aktionen des One Identity Manager Service gegen die Zielsystemumgebung ausgeführt. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet.

Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem One Identity Safeguard Konnektor installiert werden.

Detaillierte Informationen zum Thema

- Systemanforderungen für den One Identity Safeguard Synchronisationsserver auf Seite 19
- Windows PowerShell Modul safeguard-ps installieren auf Seite 20
- One Identity Manager Service mit One Identity Safeguard Konnektor installieren auf Seite 20

Systemanforderungen für den One Identity Safeguard Synchronisationsserver

Für die Einrichtung der Synchronisation mit einer One Identity Safeguard Appliance muss ein Server zur Verfügung gestellt werden, auf dem die nachfolgend genannte Software installiert ist:

- Windows Betriebssystem

  Unterstützt werden die Versionen:

    - Windows Server 2022
    - Windows Server 2019
    - Windows Server 2016
    - Windows Server 2012 R2
    - Windows Server 2012
- Microsoft .NET Framework Version 4.8 oder höher

  | HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.
- Windows PowerShell Version 5 oder höher
- Windows PowerShell Modul **safeguard-ps**

Verwandte Themen

- Windows PowerShell Modul safeguard-ps installieren auf Seite 20

Windows PowerShell Modul safeguard-ps installieren

Die Windows PowerShell Module für die unterstützten One Identity Safeguard Versionen finden Sie auf dem One Identity Manager Installationsmedium im Verzeichnis `Modules\PAG\dvd\AddOn\safeguard-ps`.

| WICHTIG: Beachten Sie, dass die Major-Version und die Minor-Version des Windows PowerShell Moduls mit der Major-Version und der Minor-Version Ihrer One Identity Safeguard Appliance übereinstimmen müssen.

Um das Windows PowerShell Modul zu installieren

1. Erstellen Sie im Verzeichnis `%ProgramFiles%\WindowsPowerShell\Modules` des Servers ein Unterverzeichnis `safeguard-ps`.
2. Kopieren Sie das Verzeichnis mit dem Windows PowerShell Modul der entsprechenden Version aus dem Verzeichnis `Modules\PAG\dvd\AddOn\safeguard-ps` des One Identity Manager Installationsmediums in das Verzeichnis `%ProgramFiles%\WindowsPowerShell\Modules\safeguard-ps` auf dem Server.

One Identity Manager Service mit One Identity Safeguard Konnektor installieren

Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem One Identity Safeguard Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein.

Tabelle 3: Eigenschaften des Jobservers

Eigenschaft	Wert
Serverfunktion	One Identity Safeguard Konnektor
Maschinenrolle	Server | Job Server | Privileged Account Management

HINWEIS: Wenn mehrere gleichartige Zielsystemumgebungen über den selben Synchronisationsserver synchronisiert werden sollen, ist es aus Performancegründen günstig, für jedes einzelne Zielsystem einen eigenen Jobserver einzurichten. Dadurch wird ein unnötiger Wechsel der Verbindungen zum Zielsystem vermieden, da stets nur gleichartige Aufträge von einem Jobserver zu verarbeiten sind (Nachnutzung bestehender Verbindungen).

Um einen Jobserver einzurichten, führen Sie folgende Schritte aus.

1. Erstellen Sie einen Jobserver und installieren und konfigurieren Sie den One Identity Manager Service.

   Um den One Identity Manager Service zu installieren, nutzen Sie das Programm Server Installer. Das Programm führt folgende Schritte aus:

   - Erstellen eines Jobservers.
   - Festlegen der Maschinenrollen und Serverfunktionen für den Jobserver.
   - Installation der One Identity Manager Service-Komponenten entsprechend der Maschinenrollen.
   - Konfigurieren des One Identity Manager Service.
   - Starten des One Identity Manager Service.

   Mit dem Server Installer können Sie den One Identity Manager Service lokal oder remote installieren.

   Für die Remote-Installation des One Identity Manager Service stellen Sie eine administrative Arbeitstation bereit, auf der die One Identity Manager-Komponenten installiert sind. Für eine lokale Installation stellen Sie sicher, dass die One Identity Manager-Komponenten auf dem Server installiert sind. Ausführliche Informationen zur Installation der One Identity Manager-Komponenten finden Sie im *One Identity Manager Installationshandbuch*.
2. Wenn Sie mit einer verschlüsselten One Identity Manager-Datenbank arbeiten, geben Sie dem One Identity Manager Service den Datenbankschlüssel bekannt. Ausführliche Informationen zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank finden Sie im *One Identity Manager Installationshandbuch*.
3. Für die Generierung von Prozessen für die Jobserver werden der Provider, Verbindungsparameter und die Authentifizierungsdaten benötigt. Diese Informationen werden im Standardfall aus den Verbindungsdaten der Datenbank ermittelt. Arbeitet der Jobserver über einen Anwendungsserver müssen Sie zusätzliche Verbindungsinformationen im Designer konfigurieren. Ausführliche Informationen zum Erfassen der Verbindungsinformationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um den One Identity Manager Service auf einem Server zu installieren und zu konfigurieren

1. Starten Sie das Programm Server Installer.

   HINWEIS: Für eine Remote-Installation starten Sie das Programm Server Installer auf Ihrer administrativen Arbeitsstation. Für eine lokale Installation starten Sie das Programm auf dem Server.

2. Auf der Seite **Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.

   Für die Verbindung zur Datenbank können Sie eine Verbindung über den Anwendungsserver oder die direkte Verbindung verwenden.

3. Auf der Seite **Servereigenschaften** legen Sie fest, auf welchem Server der One Identity Manager Service installiert werden soll.

   a. Wählen Sie in der Auswahlliste **Server** einen Jobserver aus.

      - ODER -

      Um einen neuen Jobserver zu erstellen, klicken Sie **Hinzufügen**.

   b. Bearbeiten Sie folgende Informationen für den Jobserver.

      - **Server**: Bezeichnung des Jobservers.
      - **Queue**: Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder Jobserver innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
      - **Vollständiger Servername**: Vollständiger Servername gemäß DNS Syntax.

        Syntax:

        ```
        <Name des Servers>.<Vollqualifizierter Domänenname>
        ```

   HINWEIS: Über die Option **Erweitert** können Sie weitere Eigenschaften für den Jobserver bearbeiten. Sie können die Eigenschaften auch zu einem späteren Zeitpunkt mit dem Designer bearbeiten.

4. Auf der Seite **Maschinenrollen** wählen Sie **Privileged Account Management**.
5. Auf der Seite **Serverfunktionen** wählen Sie **One Identity Safeguard Konnektor**.
6. Auf der Seite **Dienstkonfiguration** erfassen Sie die Verbindungsinformationen und prüfen Sie die Konfiguration des One Identity Manager Service.

   HINWEIS: Die initiale Konfiguration des Dienstes ist bereits vordefiniert. Sollte eine erweiterte Konfiguration erforderlich sein, können Sie diese auch zu einem späteren Zeitpunkt mit dem Designer durchführen. Ausführliche Informationen zur Konfiguration des Dienstes finden Sie im *One Identity Manager Konfigurationshandbuch*.

   Für eine direkte Verbindung zu Datenbank:

a. Wählen Sie in der Modulliste **Prozessabholung > sqlprovider**.

b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.

c. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.

d. Klicken Sie **OK**.

Für eine Verbindung zum Anwendungsserver:

a. Wählen Sie in der Modulliste den Eintrag **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen**.

b. Wählen Sie **AppServerJobProvider** und klicken Sie **OK**.

c. Wählen Sie in der Modulliste **Prozessabholung > AppServerJobProvider**.

d. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.

e. Erfassen Sie die Adresse (URL) zum Anwendungsserver und klicken Sie **OK**.

f. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.

g. Wählen Sie unter **Authentifizierungsverfahren** das Authentifizierungsmodul für die Anmeldung. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

h. Klicken Sie **OK**.

7. Zur Konfiguration der Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.
10. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.

    - **Computer**: Wählen Sie den Server über die Auswahlliste oder erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.

      Um die Installation lokal auszuführen, wählen Sie in der Auswahlliste den Eintrag **<lokale Installation>**.

    - **Dienstkonto**: Erfassen Sie die Angaben zum Benutzerkonto unter dem der One Identity Manager Service läuft. Erfassen Sie das Benutzerkonto, das Kennwort zum Benutzerkonto und die Kennwortwiederholung.

    Die Installation des Dienstes erfolgt mit dem Benutzerkonto, mit dem Sie an der administrativen Arbeitsstation angemeldet sind. Möchten Sie ein anderes Benutzerkonto für die Installation des Dienstes nutzen, können Sie dieses in den erweiterten Optionen eintragen.

Angaben zum One Identity Manager Service können Sie ebenfalls über die erweiterten Optionen ändern, beispielsweise das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den One Identity Manager Service.

11. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.

    Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.

12. Auf der letzten Seite des Server Installer klicken Sie **Fertig**.

    HINWEIS: In einer Standardinstallation wird der Dienst mit der Bezeichnung **One Identity Manager Service** in der Dienstverwaltung des Servers eingetragen.

Vorbereiten der administrativen Arbeitsstation für den Zugriff auf die One Identity Safeguard Appliance

Um im Synchronization Editor die Synchronisation mit einer One Identity Safeguard Appliance zu konfigurieren, muss der One Identity Manager Daten direkt aus der Appliance auslesen. Erfolgt der direkte Zugriff auf die Appliance von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, muss auf dieser Arbeitsstation zusätzlich die folgende Software installiert sein:

- Windows PowerShell Version 5 oder höher
- Windows PowerShell Modul **safeguard-ps**

Der an der administrativen Arbeitsstation angemeldete Benutzer benötigt im Zertifikatsspeicher des aktuellen Benutzers das Zertifikat mit dem privaten Schlüssel, das auf der One Identity Safeguard Appliance als vertrauenswürdiges Zertifikat hinterlegt ist. Das Zertifikat muss dasselbe Zertifikat sein, welches auch der Synchronisationsbenutzer verwendet. Ausführliche Informationen zu Zertifikaten im One Identity Safeguard finden Sie im *One Identity Safeguard Adminstration Guide*.

Ist der direkte Zugriff auf die Appliance von der Arbeitsstation nicht möglich, können Sie einen Remoteverbindungsserver einrichten.

Verwandte Themen

- Windows PowerShell Modul safeguard-ps installieren auf Seite 20
- Benutzer und Berechtigungen für die Synchronisation mit einer One Identity Safeguard Appliance auf Seite 17
- Vorbereiten eines Remoteverbindungsservers für den Zugriff auf die One Identity Safeguard Appliance auf Seite 25

Vorbereiten eines Remoteverbindungsservers für den Zugriff auf die One Identity Safeguard Appliance

Um die Synchronisation mit einem Zielsystem zu konfigurieren, muss der One Identity Manager Daten aus dem Zielsystem auslesen. Dabei kommuniziert der One Identity Manager direkt mit dem Zielsystem. Mitunter ist der direkte Zugriff von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, nicht möglich, beispielsweise aufgrund der Firewall-Konfiguration oder weil die Arbeitsstation nicht die notwendigen Hard- oder Softwarevoraussetzungen erfüllt. Wenn der direkte Zugriff von der Arbeitsstation nicht möglich ist, kann eine Remoteverbindung eingerichtet werden.

Der Remoteverbindungsserver und die Arbeitsstation müssen in der selben Active Directory Domäne stehen.

Konfiguration des Remoteverbindungsservers:

- One Identity Manager Service ist gestartet
- **RemoteConnectPlugin** ist installiert
- Windows PowerShell Version 5 oder höher ist installiert
- Windows PowerShell Modul **safeguard-ps** ist installiert
- One Identity Safeguard Konnektor ist installiert

Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt.

TIPP: Der Remoteverbindungsserver benötigt dieselbe Konfiguration (bezüglich der installierten Software sowie der Berechtigungen und des Zertifikates des Benutzerkontos) wie der Synchronisationsserver. Nutzen Sie den Synchronisationsserver gleichzeitig als Remoteverbindungsserver, indem Sie das **RemoteConnectPlugin** zusätzlich installieren.

Ausführliche Informationen zum Herstellen einer Remoteverbindung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Einrichten des One Identity Safeguard Synchronisationsservers auf Seite 19
- Windows PowerShell Modul safeguard-ps installieren auf Seite 20
- One Identity Manager Service mit One Identity Safeguard Konnektor installieren
- Benutzer und Berechtigungen für die Synchronisation mit einer One Identity Safeguard Appliance auf Seite 17
- Vorbereiten der administrativen Arbeitsstation für den Zugriff auf die One Identity Safeguard Appliance auf Seite 24

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer One Identity Safeguard Appliance

Verwenden Sie den Synchronization Editor, um die Synchronisation zwischen One Identity Manager-Datenbank und einer One Identity Safeguard Appliance einzurichten. Nachfolgend sind die Schritte für die initiale Einrichtung eines Synchronisationsprojektes beschrieben. Ausführliche Informationen zur Einrichtung der Synchronisation finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Nach der initialen Einrichtung können Sie innerhalb des Synchronisationsprojektes die Workflows anpassen und weitere Workflows konfigurieren. Nutzen Sie dazu den Workflow-Assistenten im Synchronization Editor. Der Synchronization Editor bietet zusätzlich verschiedene Konfigurationsmöglichkeiten für ein Synchronisationsprojekt an.

Verwandte Themen

- Benötigte Informationen für die Erstellung eines Synchronisationsprojektes auf Seite 26
- Initiales Synchronisationsprojekt für One Identity Safeguard erstellen auf Seite 28
- Vorbereiten der administrativen Arbeitsstation für den Zugriff auf die One Identity Safeguard Appliance auf Seite 24
- Vorbereiten eines Remoteverbindungsservers für den Zugriff auf die One Identity Safeguard Appliance auf Seite 25
- Einstellungen des One Identity Safeguard Konnektors auf Seite 190

Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Für die Einrichtung des Synchronisationsprojektes halten Sie die folgenden Informationen bereit.

Tabelle 4: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Hostname oder IP der Appliance	Hostname oder IP-Adresse der One Identity Safeguard Appliance. Wenn Sie einen Cluster aus mehreren One Identity Safeguard Appliances verwenden, ist hier die primäre Appliance einzutragen. HINWEIS: Dieser Wert muss angepasst werden, wenn

Angaben	Erläuterungen
	sich die primäre Appliance innerhalb des Clusters ändert. Wenn im Systemverbindungsassistenten die Option **Immer zu primärer Appliance im Cluster verbinden** aktiviert ist, wird die primäre Appliance automatisch ermittelt.
Fingerabdruck des vertrauenswürdigen Zertifikates	Fingerabdruck des vertrauenswürdigen Zertifikates, welches vom Synchronisationsbenutzer und vom Benutzerkonto des One Identity Manager Service genutzt wird. Weitere Informationen finden Sie unter Benutzer und Berechtigungen für die Synchronisation mit einer One Identity Safeguard Appliance auf Seite 17.
Synchronisationsserver für die Appliance	Vom Synchronisationsserver werden alle Aktionen des One Identity Manager Service gegen die Zielsystemumgebung ausgeführt. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet. Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem One Identity Safeguard Konnektor installiert sein. Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften. • Serverfunktion: **One Identity Safeguard Konnektor** • Maschinenrolle: **Server | Job Server | Privileged Account Management** Weitere Informationen finden Sie unter Einrichten des One Identity Safeguard Synchronisationsservers auf Seite 19.
Verbindungsdaten zur One Identity Manager-Datenbank	• Datenbankserver • Name der Datenbank • SQL Server Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung verwendet wird Die Verwendung der integrierten Windows-Authentifizierung wird nicht empfohlen. Sollten Sie das Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
Remoteverbindungsserver	Weitere Informationen finden Sie unter Vorbereiten eines

Angaben	Erläuterungen
	Remoteverbindungsservers für den Zugriff auf die One Identity Safeguard Appliance auf Seite 25.

Initiales Synchronisationsprojekt für One Identity Safeguard erstellen

HINWEIS: Der folgende Ablauf beschreibt die Einrichtung eines Synchronisationsprojekts, wenn der Synchronization Editor

- im Standardmodus ausgeführt wird und
- aus dem Launchpad gestartet wird.

Wenn der Projektassistent im Expertenmodus ausgeführt wird oder direkt aus dem Synchronization Editor gestartet wird, können zusätzliche Konfigurationseinstellungen vorgenommen werden. Folgen Sie in diesen Schritten den Anweisungen des Projektassistenten.

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

Um ein initiales Synchronisationsprojekt für One Identity Safeguard einzurichten

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.

   HINWEIS: Wenn die Synchronisation über einen Anwendungsserver ausgeführt werden soll, stellen Sie die Datenbankverbindung über den Anwendungsserver her.

2. Wählen Sie den Eintrag **Zielsystemtyp Privileged Account Management** und klicken Sie **Starten**.

   Der Projektassistent des Synchronization Editors wird gestartet.

3. Auf der Seite **Systemzugriff** legen Sie fest, wie der One Identity Manager auf das Zielsystem zugreifen kann.

   - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, möglich, nehmen Sie keine Einstellungen vor.
   - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, nicht möglich, können Sie eine Remoteverbindung herstellen.

     Aktivieren Sie die Option **Verbindung über einen Remoteverbindungsserver herstellen** und wählen Sie unter **Jobserver** den Server, über den die Verbindung hergestellt werden soll.

4. Auf der Seite **Verbindungsparameter** erfassen Sie folgende Informationen:
    - **Appliance Hostname oder IP**: Erfassen Sie den Hostname oder IP- Adresse der Appliance. Wenn Sie einen Cluster aus mehreren One Identity Safeguard Appliances verwenden, ist hier die primäre Appliance einzutragen.

      HINWEIS: Dieser Wert muss angepasst werden, wenn sich die primäre Appliance innerhalb des Clusters ändert. Wenn auf der Seite **Beschreibung der Appliance** die Option **Immer zu primärer Appliance im Cluster verbinden** aktiviert ist, wird die primäre Appliance automatisch ermittelt.
    - **Fingerabdruck des vertrauenswürdigen Zertifikates**: Erfassen Sie den Fingerabdruck des vertrauenswürdigen Zertifikates, welches vom Synchronisationsbenutzer und vom Benutzerkonto des One Identity Manager Service genutzt wird.
    - **Ignoriere SSL Verbindungsfehler**: Diese Option sollten Sie nur zu Testzwecken aktivieren, da hier potentiell Verbindungen vertraut wird, die nicht sicher sind.
    - Klicken Sie **Verbindungsdaten testen**, um die Verbindung zu testen. Es wird versucht eine Verbindung zur Appliance aufzubauen.
5. Auf der Seite **Beschreibung der Appliance** erfassen Sie folgende Informationen:
    - **Anzeigename der Appliance**:Erfassen Sie einen Anzeigenamen für die Anzeige in den One Identity Manager Werkzeugen.
    - **Systembezeichner**: Erfassen Sie einen eindeutigen Bezeichner zur Identifizierung der Appliance.

      ⚠ **VORSICHT: Der Systembezeichner muss die Appliance eindeutig beschreiben. Anhand der Systembezeichners werden die Appliances unterschieden. Die mehrfache Vergabe eines Bezeichners für unterschiedliche Appliances kann zu Fehlverhalten und Datenverlust führen.**
    - **Immer zu primärer Appliance im Cluster verbinden**: Diese Option wird automatisch gesetzt, wenn beim Testen der Verbindungsdaten ein One Identity Safeguard Cluster erkannt wird. Wenn Sie einen Cluster aus mehreren One Identity Safeguard Appliances verwenden, sollte diese Option aktiviert sein.
6. Auf der letzten Seite des Systemverbindungsassistenten können Sie die Verbindungsdaten speichern.
    - Aktivieren Sie die Option **Verbindung lokal speichern**, um die Verbindungsdaten zu speichern. Diese können Sie bei der Einrichtung weiterer Synchronisationsprojekte nutzen.
    - Um den Systemverbindungsassistenten zu beenden und zum Projektassistenten zurückzukehren, klicken Sie **Fertig**.
7. Auf der Seite **One Identity Manager Verbindung** überprüfen Sie die Verbindungsdaten zur One Identity Manager-Datenbank. Die Daten werden aus der verbundenen Datenbank geladen. Geben Sie das Kennwort erneut ein.

HINWEIS:

- Wenn Sie mit einer unverschlüsselten One Identity Manager-Datenbank arbeiten und noch kein Synchronisationsprojekt in der Datenbank gespeichert ist, erfassen Sie alle Verbindungsdaten neu.
- Wenn bereits ein Synchronisationsprojekt gespeichert ist, wird diese Seite nicht angezeigt.

8. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.
9. Auf der Seite **Zielsystemzugriff einschränken** legen Sie fest, wie der Systemzugriff erfolgen soll. Zur Auswahl stehen:

Tabelle 5: Zielsystemzugriff festlegen

Option	Bedeutung
Das Zielsystem soll nur eingelesen werden.	Gibt an, ob nur ein Synchronisationsworkflow zum initialen Einlesen des Zielsystems in die One Identity Manager-Datenbank eingerichtet werden soll. Der Synchronisationsworkflow zeigt folgende Besonderheiten: • Die Synchronisationsrichtung ist **In den One Identity Manager**. • In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung **In den One Identity Manager** definiert.
Es sollen auch Änderungen im Zielsystem durchgeführt werden.	Gibt an, ob zusätzlich zum Synchronisationsworkflow zum initialen Einlesen des Zielsystems ein Provisionierungsworkflow eingerichtet werden soll. Der Provisionierungsworkflow zeigt folgende Besonderheiten: • Die Synchronisationsrichtung ist **In das Zielsystem**. • In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung **In das Zielsystem** definiert. • Synchronisationsschritte werden nur für solche Schemaklassen erstellt, deren Schematypen schreibbar sind.

10. Auf der Seite **Synchronisationsserver** wählen Sie den Synchronisationsserver, der die Synchronisation ausführen soll.

Wenn der Synchronisationsserver noch nicht als Jobserver in der One Identity Manager-Datenbank bekannt gegeben wurde, können Sie einen neuen Jobserver anlegen.

a. Klicken Sie , um einen neuen Jobserver anzulegen.

b. Erfassen Sie die Bezeichnung des Jobservers und den vollständigen Servernamen gemäß DNS-Syntax.

c. Klicken Sie **OK**.

   Der Synchronisationsserver wird als Jobserver für das Zielsystem in der One Identity Manager-Datenbank bekannt gegeben.

d. HINWEIS: Stellen Sie nach dem Speichern des Synchronisationsprojekts sicher, dass dieser Server als Synchronisationsserver eingerichtet ist.

11. Um den Projektassistenten zu beenden, klicken Sie **Fertig**.

    Es wird ein Standardzeitplan für regelmäßige Synchronisationen erstellt und zugeordnet. Aktivieren Sie den Zeitplan für die regelmäßige Synchronisation.

    Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

    HINWEIS:

    - Beim Aktivieren wird eine Konsistenzprüfung durchgeführt. Wenn dabei Fehler auftreten, erscheint eine Meldung. Sie können entscheiden, ob das Synchronisationsprojekt dennoch aktiviert werden soll.

      Bevor Sie das Synchronisationsprojekt nutzen, prüfen Sie die Fehler. In der Ansicht **Allgemein** auf der Startseite des Synchronization Editor klicken Sie dafür **Projekt prüfen**.

    - Wenn das Synchronisationsprojekt nicht sofort aktiviert werden soll, deaktivieren Sie die Option **Synchronisationsprojekt speichern und sofort aktivieren**. In diesem Fall speichern Sie das Synchronisationsprojekt manuell vor dem Beenden des Synchronization Editor.

    - Die Verbindungsdaten zum Zielsystem werden in einem Variablenset gespeichert und können bei Bedarf im Synchronization Editor in der Kategorie **Konfiguration > Variablen** angepasst werden.

Verwandte Themen

- Benötigte Informationen für die Erstellung eines Synchronisationsprojektes auf Seite 26
- Benutzer und Berechtigungen für die Synchronisation mit einer One Identity Safeguard Appliance auf Seite 17
- Einrichten des One Identity Safeguard Synchronisationsservers auf Seite 19
- Synchronisationsprotokoll konfigurieren auf Seite 32
- Anpassen der Synchronisationskonfiguration für One Identity Safeguard auf Seite 33
- Aufgaben nach einer Synchronisation auf Seite 48
- Standardprojektvorlage für One Identity Safeguard auf Seite 187

- Einstellungen des One Identity Safeguard Konnektors auf Seite 190
- Bekannte Probleme bei der Anbindung einer One Identity Safeguard Appliance auf Seite 192

Synchronisationsprotokoll konfigurieren

Im Synchronisationsprotokoll werden alle Informationen, Hinweise, Warnungen und Fehler, die bei der Synchronisation auftreten, aufgezeichnet. Welche Informationen aufgezeichnet werden sollen, kann für jede Systemverbindung separat konfiguriert werden.

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

1. Um das Synchronisationsprotokoll für die Zielsystemverbindung zu konfigurieren, wählen Sie im Synchronization Editor die Kategorie **Konfiguration > Zielsystem**.

   - ODER -

   Um das Synchronisationsprotokoll für die Datenbankverbindung zu konfigurieren, wählen Sie im Synchronization Editor die Kategorie **Konfiguration > One Identity Manager Verbindung**.
2. Wählen Sie den Bereich **Allgemein** und klicken Sie **Konfigurieren**.
3. Wählen Sie den Bereich **Synchronisationsprotokoll** und aktivieren Sie **Synchronisationsprotokoll erstellen**.
4. Aktivieren Sie die zu protokollierenden Daten.

   HINWEIS: Einige Inhalte erzeugen besonders viele Protokolldaten. Das Synchronisationsprotokoll soll nur die für Fehleranalysen und weitere Auswertungen notwendigen Daten enthalten.
5. Klicken Sie **OK**.

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

- Aktivieren Sie im Designer den Konfigurationsparameter **DPR | Journal | LifeTime** und tragen Sie die maximale Aufbewahrungszeit ein.

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 46

Anpassen der Synchronisationskonfiguration für One Identity Safeguard

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation einer One Identity Safeguard Appliance eingerichtet. Mit diesem Synchronisationsprojekt können Sie PAM Objekte in die One Identity Manager-Datenbank einlesen. Wenn Sie Benutzerkonten und ihre Berechtigungen mit dem One Identity Manager verwalten, werden Änderungen in das Privileged Account Management System provisioniert.

HINWEIS: Wenn die Konfiguration von bereits bestehenden Synchronisationsprojekten angepasst werden soll, prüfen Sie, welche Auswirkungen die Änderungen auf die bereits synchronisierten Daten haben können.

Um die Datenbank und die One Identity Safeguard Appliance regelmäßig abzugleichen und Änderungen zu synchronisieren, passen Sie die Synchronisationskonfiguration an.

- Um bei der Synchronisation den One Identity Manager als primäres System zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um festzulegen, welche PAM Objekte und Datenbankobjekte bei der Synchronisation behandelt werden, bearbeiten Sie den Scope der Zielsystemverbindung und der One Identity Manager-Datenbankverbindung. Um Dateninkonsistenzen zu vermeiden, definieren Sie in beiden Systemen den gleichen Scope. Ist kein Scope definiert, werden alle Objekte synchronisiert.
- Um allgemeingültige Synchronisationskonfigurationen zu erstellen, die erst beim Start der Synchronisation die notwendigen Informationen über die zu synchronisierenden Objekte erhalten, können Variablen eingesetzt werden. Variablen können beispielsweise in den Basisobjekten, den Schemaklassen oder den Verarbeitungsmethoden eingesetzt werden.
- Mit Hilfe von Variablen kann ein Synchronisationsprojekt für die Synchronisation verschiedener Appliances eingerichtet werden. Hinterlegen Sie die Verbindungsparameter zur Anmeldung an der jeweiligen Appliance als Variablen.
- Wenn sich das One Identity Manager Schema oder das Zielsystemschema geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.
- Um zusätzliche Schemaeigenschaften zu synchronisieren, aktualisieren Sie das Schema im Synchronisationsprojekt. Nehmen Sie die Schemaerweiterungen in das Mapping auf.

Ausführliche Informationen zum Konfigurieren einer Synchronisation finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Detaillierte Informationen zum Thema

- Synchronisation in eine One Identity Safeguard Appliance konfigurieren auf Seite 34
- Synchronisation verschiedener One Identity Safeguard Appliances konfigurieren auf Seite 35
- Einstellungen der Systemverbindung zur One Identity Safeguard Appliance ändern auf Seite 35
- Schema aktualisieren auf Seite 39
- Provisionierung von Mitgliedschaften konfigurieren auf Seite 40
- Einzelobjektsynchronisation konfigurieren auf Seite 42
- Beschleunigung der Provisionierung und Einzelobjektsynchronisation auf Seite 43

Synchronisation in eine One Identity Safeguard Appliance konfigurieren

Das Synchronisationsprojekt für die initiale Synchronisation stellt je einen Workflow zum initialen Einlesen der Zielsystemobjekte (Initial Synchronization) und für die Provisionierung von Objektänderungen aus der One Identity Manager-Datenbank in das Zielsystem (Provisioning) bereit. Um bei der Synchronisation den One Identity Manager als primäres System zu nutzen, benötigen Sie zusätzlich einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.

Um eine Synchronisationskonfiguration für die Synchronisation in die Appliance zu erstellen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Prüfen Sie, ob die bestehenden Mappings für die Synchronisation in das Zielsystem genutzt werden können. Erstellen Sie bei Bedarf neue Mappings.
3. Erstellen Sie mit dem Workflowassistenten einen neuen Workflow.

   Es wird ein Workflow mit der Synchronisationsrichtung **In das Zielsystem** angelegt.
4. Erstellen Sie eine neue Startkonfiguration. Nutzen Sie dabei den neu angelegten Workflow.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

Verwandte Themen

- Synchronisation verschiedener One Identity Safeguard Appliances konfigurieren auf Seite 35

Synchronisation verschiedener One Identity Safeguard Appliances konfigurieren

Unter bestimmten Voraussetzungen ist es möglich ein Synchronisationsprojekt für die Synchronisation verschiedener Appliances zu nutzen.

Voraussetzungen

- Die Zielsystemschemas der Appliances sind identisch.
- Alle virtuellen Schemaeigenschaften, die im Mapping genutzt werden, müssen in den erweiterten Schemas der Appliances vorhanden sein.
- Die Verbindungsparameter zum Zielsystem sind als Variablen hinterlegt.

Um ein Synchronisationsprojekt für die Synchronisation einer weiteren Appliance anzupassen

1. Stellen Sie in der weiteren Appliance einen Benutzer mit ausreichenden Berechtigungen bereit.
2. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
3. Erstellen Sie für die Appliance ein neues Basisobjekt.
    - Verwenden Sie den Assistenten zur Anlage eines Basisobjektes.
    - Wählen Sie im Assistenten den One Identity Safeguard Konnektor.
    - Geben Sie die Verbindungsparameter bekannt. Die Verbindungsparameter werden in einem spezialisierten Variablenset gespeichert.

    Es wird eine Startkonfiguration erstellt, die das neu angelegte Variablenset verwendet.
4. Passen Sie bei Bedarf weitere Komponenten der Synchronisationskonfiguration an.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

Verwandte Themen

- Synchronisation in eine One Identity Safeguard Appliance konfigurieren auf Seite 34

Einstellungen der Systemverbindung zur One Identity Safeguard Appliance ändern

Beim Einrichten der initialen Synchronisation werden für die Eigenschaften der Systemverbindung Standardwerte gesetzt. Diese Standardwerte können angepasst werden. Dafür gibt es zwei Wege:

a. Legen Sie ein spezialisiertes Variablenset an und ändern Sie die Werte der betroffenen Variablen.

   Die Standardwerte bleiben im Standardvariablenset erhalten. Die Variablen können jederzeit auf die Standardwerte zurückgesetzt werden. (Empfohlenes Vorgehen)

b. Bearbeiten Sie die Zielsystemverbindung mit dem Systemverbindungsassistenten und ändern Sie die betroffenen Werte.

   Der Systemverbindungsassistent liefert zusätzliche Erläuterungen zu den Einstellungen. Die Standardwerte können nur unter bestimmten Voraussetzungen wiederhergestellt werden.

Detaillierte Informationen zum Thema

- Verbindungsparameter im Variablenset bearbeiten auf Seite 36
- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 37
- Anpassen der Windows PowerShell Definition des One Identity Safeguard Konnektors auf Seite 38
- Einstellungen des One Identity Safeguard Konnektors auf Seite 190

Verbindungsparameter im Variablenset bearbeiten

Die Verbindungsparameter wurden beim Einrichten der Synchronisation als Variablen im Standardvariablenset gespeichert. Sie können die Werte dieser Variablen in einem spezialisierten Variablenset Ihren Erfordernissen anpassen und dieses Variablenset einer Startkonfiguration und einem Basisobjekt zuordnen. Damit haben Sie jederzeit die Möglichkeit, erneut die Standardwerte aus dem Standardvariablenset zu nutzen.

HINWEIS: Um die Datenkonsistenz in den angebundenen Zielsystemen zu bewahren, stellen Sie sicher, dass die Startkonfiguration für die Synchronisation und das Basisobjekt für die Provisionierung dasselbe Variablenset verwenden. Das gilt insbesondere, wenn ein Synchronisationsprojekt für die Synchronisation verschiedener One Identity Safeguard Appliances genutzt wird.

Um die Verbindungsparameter in einem spezialisierten Variablenset anzupassen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
3. Öffnen Sie die Ansicht **Verbindungsparameter**.

   Einige Verbindungsparameter können hier in Variablen umgewandelt werden. Für andere sind bereits Variablen angelegt.
4. Wählen Sie einen Parameter und klicken Sie **Umwandeln**.
5. Wählen Sie die Kategorie **Konfiguration > Variablen**.

Im unteren Bereich der Dokumentenansicht werden alle spezialisierten Variablensets angezeigt.

6. Wählen Sie ein spezialisiertes Variablenset oder klicken Sie in der Symbolleiste der Variablensetansicht .
   - Um das Variablenset umzubenennen, markieren Sie das Variablenset und klicken Sie in der Symbolleiste der Variablensetansicht . Erfassen Sie einen Namen für das Variablenset.
7. Wählen Sie die zuvor angelegten Variablen und erfassen Sie neue Werte.
8. Wählen Sie die Kategorie **Konfiguration > Startkonfigurationen**.
9. Wählen Sie eine Startkonfiguration und klicken Sie **Bearbeiten**.
10. Wählen Sie den Tabreiter **Allgemein**.
11. Ordnen Sie im Eingabefeld **Variablenset** das spezialisierte Variablenset zu.
12. Wählen Sie die Kategorie **Konfiguration > Basisobjekte**.
13. Wählen Sie ein Basisobjekt und klicken Sie .

    - ODER -

    Klicken Sie , um ein neues Basisobjekt anzulegen.
14. Ordnen Sie im Eingabefeld **Variablenset** das spezialisierte Variablenset zu.
15. Speichern Sie die Änderungen.

Ausführliche Informationen zur Anwendung von Variablen und Variablensets, zum Wiederherstellen der Standardwerte und zum Anlegen von Basisobjekten finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 37

Eigenschaften der Zielsystemverbindung bearbeiten

Die Verbindungsparameter können auch mit dem Systemverbindungsassistenten geändert werden. Wenn für die Einstellungen Variablen definiert sind, werden die Änderungen in das aktive Variablenset übernommen.

HINWEIS: Unter folgenden Umständen können die Standardwerte nicht wiederhergestellt werden:

- Die Verbindungsparameter sind nicht als Variablen hinterlegt.
- Das Standardvariablenset ist als aktives Variablenset ausgewählt.

In beiden Fällen überschreibt der Systemverbindungsassistent die Standardwerte. Sie können später nicht wiederhergestellt werden.

Um die Verbindungsparameter mit dem Systemverbindungsassistenten zu bearbeiten

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie in der Symbolleiste das aktive Variablenset, das für die Verbindung zum Zielsystem verwendet werden soll.

   HINWEIS: Ist das Standardvariablenset ausgewählt, werden die Standardwerte überschrieben und können später nicht wiederhergestellt werden.
3. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
4. Klicken Sie **Verbindung bearbeiten**.

   Der Systemverbindungsassistent wird gestartet.
5. Folgen Sie den Anweisungen des Systemverbindungsassistenten und ändern Sie die gewünschten Eigenschaften.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Verbindungsparameter im Variablenset bearbeiten auf Seite 36

Anpassen der Windows PowerShell Definition des One Identity Safeguard Konnektors

Mit dieser Einstellung können Sie die Definition anpassen, die vom One Identity Safeguard Konnektor verwendet wird.

WICHTIG: Die Konnektordefinition sollte nur mit Anweisungen eines Support-Mitarbeiters geändert werden. Änderungen an dieser Einstellung haben weitreichende Auswirkungen in der Synchronisation und müssen deshalb sehr vorsichtig behandelt werden.

HINWEIS: Eine angepasste Konnektordefinition wird nicht standardmäßig überschrieben, wenn eine neue Version des Konnektors beziehungsweise eine aktualisierte Konnektordefinition herausgegeben wird.

Um die Konnektordefinition anzupassen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
3. Klicken Sie **Verbindung bearbeiten**.

   Der Systemverbindungsassistent wird gestartet.
4. Auf der Startseite des Systemverbindungsassistenten aktivieren Sie **Erweiterte Einstellungen anzeigen**.
5. Auf der Seite **Erweiterte Einstellungen** passen Sie die Konnektordefinition an.

a. Wählen Sie die Option **Konnektordefinition anpassen**.

b. Bearbeiten Sie die Definition in Absprache mit dem Support-Mitarbeiter. Sie können folgende Aktionen ausführen:

- Mit laden Sie die Definition aus einer Datei.
- Mit prüfen Sie die Definition auf Fehler.
- Mit zeigen Sie die Unterschiede zur Standardversion an.

6. Folgen Sie den weiteren Anweisungen des Systemverbindungsassistenten.
7. Speichern Sie die Änderungen.

Schema aktualisieren

Während ein Synchronisationsprojekt bearbeitet wird, stehen alle Schemadaten (Schematypen und Schemaeigenschaften) des Zielsystemschemas und des One Identity Manager Schemas zur Verfügung. Für eine Synchronisationskonfiguration wird jedoch nur ein Teil dieser Daten benötigt. Wenn ein Synchronisationsprojekt fertig gestellt wird, werden die Schemas komprimiert, um die nicht benötigten Daten aus dem Synchronisationsprojekt zu entfernen. Dadurch kann das Laden des Synchronisationsprojekts beschleunigt werden. Die entfernten Schemadaten können zu einem späteren Zeitpunkt wieder in die Synchronisationskonfiguration aufgenommen werden.

Wenn sich das Zielsystemschema oder das One Identity Manager Schema geändert hat, müssen diese Änderungen ebenfalls in die Synchronisationskonfiguration aufgenommen werden. Anschließend können die Änderungen in das Mapping der Schemaeigenschaften eingearbeitet werden.

Um Schemadaten, die beim Komprimieren entfernt wurden, und Schemaänderungen in der Synchronisationskonfiguration berücksichtigen zu können, aktualisieren Sie das jeweilige Schema im Synchronisationsprojekt. Das kann erforderlich sein, wenn:

- ein Schema geändert wurde, durch:
  - Änderungen am Zielsystemschema
  - unternehmensspezifische Anpassungen des One Identity Manager Schemas
  - eine Update-Migration des One Identity Manager
- ein Schema im Synchronisationsprojekt komprimiert wurde, durch:
  - die Aktivierung des Synchronisationsprojekts
  - erstmaliges Speichern des Synchronisationsprojekts
  - Komprimieren eines Schemas

Um das Schema einer Systemverbindung zu aktualisieren

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.

- ODER -

Wählen Sie die Kategorie **Konfiguration > One Identity Manager Verbindung**.

3. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Die Schemadaten werden neu geladen.

Um ein Mapping zu bearbeiten

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Mappings**.
3. Wählen Sie in der Navigationsansicht das Mapping.

   Der Mappingeditor wird geöffnet. Ausführliche Informationen zum Bearbeiten von Mappings finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

HINWEIS: Wenn das Schema eines aktivierten Synchronisationsprojekts aktualisiert wird, wird das Synchronisationsprojekt deaktiviert. Damit Synchronisationen ausgeführt werden, aktivieren Sie das Synchronisationsprojekt erneut.

Beschleunigung der Synchronisation durch Revisionsfilterung

Die Synchronisation mit einer One Identity Safeguard Appliance unterstützt keine Revisionsfilterung.

Provisionierung von Mitgliedschaften konfigurieren

Mitgliedschaften, beispielsweise von Benutzerkonten in Gruppen, werden in der One Identity Manager-Datenbank in Zuordnungstabellen gespeichert. Bei der Provisionierung von geänderten Mitgliedschaften werden möglicherweise Änderungen, die im Zielsystem vorgenommen wurden, überschrieben. Dieses Verhalten kann unter folgenden Bedingungen auftreten:

- Mitgliedschaften werden im Zielsystem in Form einer Liste als Eigenschaft eines Objekts gespeichert.

  Beispiel: Liste von Benutzern in der Eigenschaft `Users` einer PAM Benutzergruppe (`UserGroup`)
- Änderungen von Mitgliedschaften sind in beiden verbundenen Systemen zulässig.
- Ein Provisionierungsworkflow und Provisionierungsprozesse sind eingerichtet.

Wird eine Mitgliedschaft im One Identity Manager geändert, wird standardmäßig die komplette Mitgliederliste in das Zielsystem übertragen. Mitgliedschaften, die zuvor im Zielsystem hinzugefügt wurden, werden dabei entfernt; zuvor gelöschte Mitgliedschaften werden wieder eingefügt.

Um das zu verhindern, kann die Provisionierung so konfiguriert werden, dass nur die einzelne geänderte Mitgliedschaft in das Zielsystem provisioniert wird. Das entsprechende Verhalten wird für jede Zuordnungstabelle separat konfiguriert.

Um die Einzelprovisionierung von Mitgliedschaften zu ermöglichen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Privileged Account Management**.
3. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
4. Wählen Sie die Zuordnungstabellen, für die Sie die Einzelprovisionierung ermöglichen möchten. Mehrfachauswahl ist möglich.
5. Klicken Sie **Merge-Modus**.

   HINWEIS:

   - Die Option kann nur für Zuordnungstabellen aktiviert werden, deren Basistabelle eine Spalte `XDateSubItem` hat.
   - Zuordnungstabellen, die im Mapping in einer virtuellen Schemaeigenschaft zusammengefasst sind, müssen identisch markiert werden.
6. Speichern Sie die Änderungen.

Für jede Zuordnungstabelle, die so gekennzeichnet ist, werden Änderungen, die im One Identity Manager vorgenommen werden, in einer separaten Tabelle gespeichert. Dabei werden nur die neu eingefügten und gelöschten Zuordnungen verarbeitet. Bei der Provisionierung der Änderungen wird die Mitgliederliste im Zielsystem mit den Einträgen in dieser Tabelle abgeglichen. Damit wird nicht die gesamte Mitgliederliste überschrieben, sondern nur die einzelne geänderte Mitgliedschaft provisioniert.

HINWEIS: Bei einer Synchronisation wird immer die komplette Mitgliederliste aktualisiert. Dabei werden Objekte mit Änderungen, deren Provisionierung noch nicht abgeschlossen ist, nicht verarbeitet. Diese Objekte werden im Synchronisationsprotokoll aufgezeichnet.

Die Einzelprovisionierung von Mitgliedschaften kann durch eine Bedingung eingeschränkt werden. Wenn für eine Tabelle der Merge-Modus deaktiviert wird, dann wird auch die Bedingung gelöscht. Tabellen, bei denen die Bedingung bearbeitet oder gelöscht wurde, sind durch folgendes Symbol gekennzeichnet:  . Die originale Bedingung kann jederzeit wiederhergestellt werden.

Um die originale Bedingung wiederherzustellen

1. Wählen Sie die Zuordnungstabelle, für welche Sie die Bedingung wiederherstellen möchten.

2. Klicken Sie mit der rechten Maustaste auf die gewählte Zeile und wählen Sie im Kontextmenü **Originalwerte wiederherstellen**.
3. Speichern Sie die Änderungen.

HINWEIS: Um in der Bedingung den Bezug zu den eingefügten oder gelöschten Zuordnungen herzustellen, nutzen Sie den Tabellenalias `i`.

Beispiel für eine Bedingung an der Zuordnungstabelle `PAGUserInUsrGroup`:

```
exists (select top 1 1 from PAGUsrGroup g
     where g.UID_PAGUsrGroup = i.UID_PAGUsrGroup
     and <einschränkende Bedingung>)
```

Ausführliche Informationen zur Provisionierung von Mitgliedschaften finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Einzelobjektsynchronisation konfigurieren

Änderungen an einem einzelnen Objekt im Zielsystem können sofort in die One Identity Manager-Datenbank übertragen werden, ohne dass eine vollständige Synchronisation der Zielsystem-Umgebung gestartet werden muss. Die Einzelobjektsynchronisation kann nur für Objekte ausgeführt werden, die in der One Identity Manager-Datenbank bereits vorhanden sind. Es werden die Änderungen an den gemappten Objekteigenschaften übernommen. Gehört zu diesen Objekteigenschaften eine Mitgliederliste, werden auch die Einträge in der Zuordnungstabelle aktualisiert. Ist das Objekt im Zielsystem nicht mehr vorhanden, wird es in der One Identity Manager-Datenbank gelöscht.

Voraussetzungen

- Es gibt einen Synchronisationsschritt, der die Änderungen am geänderten Objekt in den One Identity Manager einlesen kann.
- Für die Tabelle, die das geänderte Objekt enthält, ist der Pfad zum Basisobjekt der Synchronisation festgelegt.

Für Synchronisationsprojekte, die mit der Standard-Projektvorlage erstellt wurden, ist die Einzelobjektsynchronisation vollständig konfiguriert. Wenn Sie kundenspezifische Tabellen in solch ein Synchronisationsprojekt einbeziehen möchten, müssen Sie die Einzelobjektsynchronisation für diese Tabellen konfigurieren. Ausführliche Informationen dazu finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Um den Pfad zum Basisobjekt der Synchronisation für eine kundenspezifische Tabelle festzulegen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Privileged Account Management**.

3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die kundenspezifische Tabelle zu, für die Sie die Einzelobjektsynchronisation nutzen möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die kundenspezifische Tabelle und erfassen Sie den **Pfad zum Basisobjekt**.

   Geben Sie den Pfad zum Basisobjekt in der ObjectWalker-Notation der VI.DB an.

   Beispiel: `FK(UID_PAGAppliance).XObjectKey`
8. Speichern Sie die Änderungen.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 47
- Ausstehende Objekte nachbearbeiten auf Seite 49

Beschleunigung der Provisionierung und Einzelobjektsynchronisation

Um Lastspitzen aufzufangen, kann die Verarbeitung der Prozesse zur Provisionierung und Einzelobjektsynchronisation auf mehrere Jobserver verteilt werden. Damit können die Provisionierung und Einzelobjektsynchronisation beschleunigt werden.

HINWEIS: Die Lastverteilung sollte nicht permanent für Provisionierungen oder Einzelobjektsynchronisationen eingesetzt werden. Durch die parallele Verarbeitung der Objekte kann es beispielsweise vorkommen, dass Abhängigkeiten nicht aufgelöst werden, da die referenzierten Objekte von einem anderen Jobserver noch nicht vollständig verarbeitet wurden.

Sobald die Lastverteilung nicht mehr benötigt wird, stellen Sie sicher, dass der Synchronisationsserver die Prozesse zur Provisionierung und Einzelobjektsynchronisation ausführt.

Um die Lastverteilung zu konfigurieren

1. Konfigurieren Sie die Server und geben Sie diese im One Identity Manager als Jobserver bekannt.
   - Für Jobserver, die an der Lastverteilung teilnehmen, muss die Option **Keine Prozesszuteilung** deaktiviert sein.
   - Weisen Sie diesen Jobservern die Serverfunktion **One Identity Safeguard Konnektor** zu.

   Alle Jobserver müssen auf die jeweilige Appliance zugreifen können, wie der Synchronisationsserver für das jeweilige Basisobjekt.

2. Weisen Sie im Synchronization Editor an das Basisobjekt eine kundendefinierte Serverfunktion zu.

   Über diese Serverfunktion werden alle Jobserver identifiziert, welche für die Lastverteilung genutzt werden sollen.

   Wenn für das Basisobjekt noch keine kundendefinierte Serverfunktion vorhanden ist, erstellen Sie hier eine neue.

   Ausführliche Informationen zur Bearbeitung von Basisobjekten finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

3. Weisen Sie diese Serverfunktion im Manager an alle Jobserver zu, welche die Prozesse zur Provisionierung und Einzelobjektsynchronisation für das Basisobjekt verarbeiten sollen.

   Wählen Sie nur die Jobserver, welche die gleiche Konfiguration wie der Synchronisationsserver des Basisobjekts haben.

Sobald alle Prozesse verarbeitet wurden, soll wieder der Synchronisationsserver die Provisionierung und Einzelobjektsynchronisation ausführen.

Um den Synchronisationsserver ohne Lastverteilung zu nutzen

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

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

Detaillierte Informationen zum Thema

- PAM Jobserver bearbeiten auf Seite 178

Ausführen einer Synchronisation

Synchronisationen werden über zeitgesteuerte Prozessaufträge gestartet. Im Synchronization Editor ist es auch möglich, eine Synchronisation manuell zu starten. Zuvor können Sie die Synchronisation simulieren, um das Ergebnis der Synchronisation abzuschätzen und Fehler in der Synchronisationskonfiguration aufzudecken. Wenn eine Synchronisation irregulär abgebrochen wurde, müssen Sie die Startinformation zurücksetzen, um die Synchronisation erneut starten zu können.

Wenn verschiedene Zielsysteme immer in einer vorher festgelegten Reihenfolge synchronisiert werden sollen, nutzen Sie Startfolgen, um die Synchronisation zu starten. In einer Startfolge können beliebige Startkonfigurationen aus verschiedenen Synchronisationsprojekten zusammengestellt und in eine Ausführungsreihenfolge gebracht werden. Ausführliche Informationen zu Startfolgen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Detaillierte Informationen zum Thema

- Synchronisationen starten auf Seite 45
- Synchronisationsergebnisse anzeigen auf Seite 46
- Synchronisation deaktivieren auf Seite 47
- Einzelobjekte synchronisieren auf Seite 47
- Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) auf Seite 53

Synchronisationen starten

Beim Einrichten des initialen Synchronisationsprojekts über das Launchpad werden Standardzeitpläne für regelmäßige Synchronisationen erstellt und zugeordnet. Um regelmäßige Synchronisationen auszuführen, aktivieren Sie diese Zeitpläne.

Um regelmäßige Synchronisationen auszuführen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Startkonfigurationen**.
3. Wählen Sie in der Dokumentenansicht eine Startkonfiguration aus und klicken Sie **Zeitplan bearbeiten**.
4. Bearbeiten Sie die Eigenschaften des Zeitplans.
5. Um den Zeitplan zu aktivieren, klicken Sie **Aktiviert**.
6. Klicken Sie **OK**.

Wenn kein Zeitplan aktiviert ist, können Sie die Synchronisation auch manuell starten.

Um die initiale Synchronisation manuell zu starten

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Startkonfigurationen**.
3. Wählen Sie in der Dokumentenansicht eine Startkonfiguration und klicken Sie **Ausführen**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

WICHTIG: Solange eine Synchronisation ausgeführt wird, sollte keine weitere Synchronisation für dasselbe Zielsystem gestartet werden. Das gilt insbesondere, wenn dieselben Synchronisationsobjekte verarbeitet werden.

- Wenn eine weitere Synchronisation mit derselben Startkonfiguration gestartet wird, wird dieser Prozess gestoppt und erhält den Ausführungsstatus **Frozen**. Es wird eine Fehlermeldung in die Protokolldatei des One Identity Manager Service geschrieben.

    - Stellen Sie sicher, dass Startkonfigurationen, die in Startfolgen verwendet werden, nicht gleichzeitig einzeln gestartet werden. Weisen Sie den Startfolgen und Startkonfigurationen unterschiedliche Zeitpläne zu.
- Wenn eine weitere Synchronisation mit einer anderen Startkonfiguration gestartet wird, die dasselbe Zielsystem anspricht, kann das zu Synchronisationsfehlern oder Datenverlust führen. Legen Sie an den Startkonfigurationen fest, wie sich der One Identity Manager in diesem Fall verhalten soll.
    - Stellen Sie über den Zeitplan sicher, dass die Startkonfigurationen nacheinander ausgeführt werden.
    - Gruppieren Sie die Startkonfigurationen mit gleichem Startverhalten.

Synchronisationsergebnisse anzeigen

Die Ergebnisse der Synchronisation werden im Synchronisationsprotokoll zusammengefasst. Der Umfang des Synchronisationsprotokolls kann für jede Systemverbindung separat festgelegt werden. Der One Identity Manager stellt verschiedene Berichte bereit, in denen die Synchronisationsergebnisse nach verschiedenen Kriterien aufbereitet sind.

Um das Protokoll einer Synchronisation anzuzeigen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Protokolle**.
3. Klicken Sie in der Symbolleiste der Navigationsansicht .

   In der Navigationsansicht werden die Protokolle aller abgeschlossenen Synchronisationsläufe angezeigt.
4. Wählen Sie per Maus-Doppelklick das Protokoll, das angezeigt werden soll.

   Die Auswertung der Synchronisation wird als Bericht angezeigt. Sie können diesen Bericht speichern.

Um das Protokoll einer Provisionierung anzuzeigen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Protokolle**.
3. Klicken Sie in der Symbolleiste der Navigationsansicht .

   In der Navigationsansicht werden die Protokolle aller abgeschlossenen Provisionierungsprozesse angezeigt.
4. Wählen Sie per Maus-Doppelklick das Protokoll, das angezeigt werden soll.

   Die Auswertung der Provisionierung wird als Bericht angezeigt. Sie können diesen Bericht speichern.

Die Protokolle sind in der Navigationsansicht farblich gekennzeichnet. Die Kennzeichnung gibt den Ausführungsstatus der Synchronisation/Provisionierung wieder.

TIPP: Die Protokolle werden auch im Manager unter der Kategorie **<Zielsystemtyp> > Synchronisationsprotokolle** angezeigt.

Verwandte Themen

- Synchronisationsprotokoll konfigurieren auf Seite 32
- Fehleranalyse auf Seite 52

Synchronisation deaktivieren

Regelmäßige Synchronisationen können nur gestartet werden, wenn das Synchronisationsprojekt und der Zeitplan aktiviert sind.

Um regelmäßige Synchronisationen zu verhindern

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Startkonfiguration und deaktivieren Sie den hinterlegten Zeitplan.

   Synchronisationen können nun nur noch manuell gestartet werden.

Ein aktiviertes Synchronisationsprojekt kann nur eingeschränkt bearbeitet werden. Sind Schemaänderungen notwendig, muss das Schema im Synchronisationsprojekt aktualisiert werden. Dabei wird das Synchronisationsprojekt deaktiviert und kann erneut bearbeitet werden.

Des Weiteren muss das Synchronisationsprojekt deaktiviert werden, wenn keinerlei Synchronisationen gestartet werden dürfen (auch nicht manuell).

Um das Synchronisationsprojekt zu deaktivieren

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie auf der Startseite die Ansicht **Allgemein**.
3. Klicken Sie **Projekt deaktivieren**.

Verwandte Themen

- Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) auf Seite 53

Einzelobjekte synchronisieren

Die Einzelobjektsynchronisation kann nur für Objekte ausgeführt werden, die in der One Identity Manager-Datenbank bereits vorhanden sind. Es werden die Änderungen an den gemappten Objekteigenschaften übernommen. Gehört zu diesen Objekteigenschaften eine Mitgliederliste, werden auch die Einträge in der Zuordnungstabelle aktualisiert.

HINWEIS: Ist das Objekt im Zielsystem nicht mehr vorhanden, wird es in der One Identity Manager-Datenbank gelöscht.

Um ein Einzelobjekt zu synchronisieren

1. Wählen Sie im Manager die Kategorie **Privileged Account Management**.
2. Wählen Sie in der Navigationsansicht den Objekttyp.
3. Wählen Sie in der Ergebnisliste das Objekt, das Sie synchronisieren möchten.
4. Wählen Sie die Aufgabe **Objekt synchronisieren**.

   Es wird ein Prozess zum Lesen dieses Objekts in die Jobqueue eingestellt.

Besonderheiten bei der Synchronisation von Mitgliederlisten

Wenn Sie Änderungen in der Mitgliederliste eines Objekts synchronisieren, führen Sie die Einzelobjektsynchronisation am Basisobjekt der Zuweisung aus. Die Basistabelle einer Zuordnung enthält eine Spalte `XDateSubItem` mit der Information über die letzte Änderung der Mitgliedschaften.

Beispiel:

Basisobjekt für die Zuweisung von PAM Benutzerkonten an PAM Benutzergruppen ist die Benutzergruppe.

Im Zielsystem wurde ein Benutzerkonto an eine Gruppe zugewiesen. Um diese Zuweisung zu synchronisieren, wählen Sie im Manager die Gruppe, der das Benutzerkonto zugewiesen wurde, und führen Sie die Einzelobjektsynchronisation aus. Dabei werden alle Mitgliedschaften für diese Gruppe synchronisiert.

Das Benutzerkonto muss in der One Identity Manager-Datenbank bereits als Objekt vorhanden sein, damit die Zuweisung angelegt werden kann.

Detaillierte Informationen zum Thema

- Einzelobjektsynchronisation konfigurieren auf Seite 42

Aufgaben nach einer Synchronisation

Nach der Synchronisation von Daten aus dem Zielsystem in die One Identity Manager-Datenbank können Nacharbeiten erforderlich sein. Prüfen Sie folgende Aufgaben:

- Ausstehende Objekte nachbearbeiten auf Seite 49
- Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen auf Seite 51
- PAM Benutzerkonten über Kontendefinitionen verwalten auf Seite 51

Ausstehende Objekte nachbearbeiten

Objekte, die im Zielsystem nicht vorhanden sind, können bei der Synchronisation in den One Identity Manager als ausstehend gekennzeichnet werden. Damit kann verhindert werden, dass Objekte aufgrund einer fehlerhaften Datensituation oder einer fehlerhaften Synchronisationskonfiguration gelöscht werden.

Ausstehende Objekte

- können im One Identity Manager nicht bearbeitet werden,
- werden bei jeder weiteren Synchronisation ignoriert,
- werden bei der Vererbungsberechnung ignoriert.

Das heißt, sämtliche Mitgliedschaften und Zuweisungen bleiben solange erhalten, bis die ausstehenden Objekte nachbearbeitet wurden.

Führen Sie dafür einen Zielsystemabgleich durch.

Um ausstehende Objekte nachzubearbeiten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Zielsystemabgleich: Privileged Account Management**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp **Privileged Account Management** als Synchronisationstabellen zugewiesen sind.
2. Öffnen Sie auf dem Formular **Zielsystemabgleich**, in der Spalte **Tabelle/Objekt** den Knoten der Tabelle, für die sie ausstehende Objekte nachbearbeiten möchten.

   Es werden alle Objekte angezeigt, die als ausstehend markiert sind. Die Spalten **Letzter Protokolleintrag** und **Letzte ausgeführte Methode** zeigen den Zeitpunkt für den letzten Eintrag im Synchronisationsprotokoll und die dabei ausgeführte Verarbeitungsmethode. Der Eintrag **Kein Protokoll verfügbar** hat folgende Bedeutungen:

   - Das Synchronisationsprotokoll wurde bereits gelöscht.

     - ODER -
   - Im Zielsystem wurde eine Zuweisung aus einer Mitgliederliste gelöscht.

     Bei der Synchronisation wird das Basisobjekt der Zuordnung aktualisiert. Dafür erscheint ein Eintrag im Synchronisationsprotokoll. Der Eintrag in der Zuordnungstabelle wird als ausstehend markiert, es gibt jedoch keinen Eintrag im Synchronisationsprotokoll.
   - Im Zielsystem wurde ein Objekt gelöscht, das eine Mitgliederliste enthält.

     Bei der Synchronisation werden das Objekt und alle zugehörigen Einträge in Zuordnungstabellen als ausstehend markiert. Ein Eintrag im Synchronisationsprotokoll erscheint jedoch nur für das gelöschte Objekt.

   TIPP:

Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

1. Wählen Sie auf dem Formular für den Zielsystemabgleich das Objekt.
2. Öffnen Sie das Kontextmenü und klicken Sie **Objekt anzeigen**.

3. Wählen Sie die Objekte, die Sie nachbearbeiten möchten. Mehrfachauswahl ist möglich.
4. Klicken Sie in der Formularsymbolleiste eins der folgenden Symbole, um die jeweilige Methode auszuführen.

Tabelle 6: Methoden zur Behandlung ausstehender Objekte

Symbol	Methode	Beschreibung
	Löschen	Das Objekt wird sofort in der One Identity Manager-Datenbank gelöscht. Eine Löschverzögerung wird nicht berücksichtigt. Indirekte Mitgliedschaften können nicht gelöscht werden.
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung **Ausstehend** wird für das Objekt entfernt. Es wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt. Voraussetzungen: • Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen. • Der Zielsystemkonnektor kann schreibend auf das Zielsystem zugreifen.
	Zurücksetzen	Die Markierung **Ausstehend** wird für das Objekt entfernt.

5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

HINWEIS: Standardmäßig werden die ausgewählten Objekte parallel verarbeitet. Damit wird die Ausführung der ausgewählten Methode beschleunigt. Wenn bei der Verarbeitung ein Fehler auftritt, wird die Aktion abgebrochen und alle Änderungen werden rückgängig gemacht.

Um den Fehler zu lokalisieren, muss die Massenverarbeitung der Objekte deaktiviert werden. Die Objekte werden damit nacheinander verarbeitet. Das fehlerhafte Objekt wird in der Fehlermeldung benannt. Alle Änderungen, die bis zum Auftreten des Fehlers vorgenommen wurden, werden gespeichert.

Um die Massenverarbeitung zu deaktivieren

- Deaktivieren Sie in der Formularsymbolleiste das Symbol .

HINWEIS: Damit ausstehende Objekte in der Nachbehandlung publiziert werden können, muss der Zielsystemkonnektor schreibend auf das Zielsystem zugreifen können. Das heißt, an der Zielsystemverbindung ist die Option **Verbindung darf nur gelesen werden** deaktiviert.

Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen

Für die Synchronisation in kundenspezifische Tabellen müssen Sie den Zielsystemabgleich anpassen.

Um kundenspezifische Tabellen in den Zielsystemabgleich aufzunehmen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Privileged Account Management**.
3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die kundenspezifischen Tabellen zu, für die Sie ausstehende Objekte behandeln möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die kundenspezifischen Tabellen, für die ausstehende Objekte in das Zielsystem publiziert werden dürfen und aktivieren Sie die Option **Publizierbar**.
8. Speichern Sie die Änderungen.

Verwandte Themen

- Ausstehende Objekte nachbearbeiten auf Seite 49

PAM Benutzerkonten über Kontendefinitionen verwalten

Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Personen erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für die Appliance bekannt, werden die Benutzerkonten mit den Personen verbunden. Es wird jedoch noch keine Kontendefinition zugewiesen. Die Benutzerkonten sind somit im Zustand **Linked** (verbunden).

Um die Benutzerkonten über Kontendefinitionen zu verwalten, weisen Sie diesen Benutzerkonten eine Kontendefinition und einen Automatisierungsgrad zu.

Detaillierte Informationen zum Thema

- Kontendefinitionen an verbundene PAM Benutzerkonten zuweisen auf Seite 84

Fehleranalyse

Bei der Analyse und Behebung von Synchronisationsfehlern unterstützt Sie der Synchronization Editor auf verschiedene Weise.

- Synchronisation simulieren

  Die Simulation ermöglicht es, das Ergebnis einer Synchronisation abzuschätzen. Dadurch können beispielsweise Fehler in der Synchronisationskonfiguration aufgedeckt werden.

- Synchronisation analysieren

  Für die Analyse von Problemen während der Synchronisation, beispielsweise unzureichender Performance, kann der Synchronisationsanalysebericht erzeugt werden.

- Meldungen protokollieren

  Der One Identity Manager bietet verschiedene Möglichkeiten zur Protokollierung von Meldungen. Dazu gehören das Synchronisationsprotokoll, die Protokolldatei des One Identity Manager Service, die Protokollierung von Meldungen mittels NLog und weitere.

- Startinformation zurücksetzen

  Wenn eine Synchronisation irregulär abgebrochen wurde, beispielsweise weil ein Server nicht erreichbar war, muss die Startinformation manuell zurückgesetzt werden. Erst danach kann die Synchronisation erneut gestartet werden.

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

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 46

Datenfehler bei der Synchronisation ignorieren

Standardmäßig werden Objekte mit fehlerhaften Daten nicht synchronisiert. Diese Objekte können synchronisiert werden, sobald die fehlerhaften Daten korrigiert wurden. In einzelnen Situationen kann es notwendig sein, solche Objekte dennoch zu synchronisieren

und nur die fehlerhaften Objekteigenschaften zu ignorieren. Dieses Verhalten kann für die Synchronisation in den One Identity Manager konfiguriert werden.

Um Datenfehler bei der Synchronisation in den One Identity Manager zu ignorieren

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > One Identity Manager Verbindung**.
3. In der Ansicht **Allgemein** klicken Sie **Verbindung bearbeiten**.

   Der Systemverbindungsassistent wird gestartet.
4. Auf der Seite **Weitere Einstellungen** aktivieren Sie **Versuche Datenfehler zu ignorieren**.

   Diese Option ist nur wirksam, wenn am Synchronisationsworkflow **Bei Fehler fortsetzen** eingestellt ist.

   Fehler in Standardspalten, wie Primärschlüssel oder UID-Spalten, und Pflichteingabespalten können nicht ignoriert werden.
5. Speichern Sie die Änderungen.

WICHTIG: Wenn die Option aktiviert ist, versucht der One Identity Manager Speicherfehler zu ignorieren, die auf Datenfehler in einer einzelnen Spalte zurückgeführt werden können. Dabei wird die Datenänderung an der betroffenen Spalte verworfen und das Objekt anschließend neu gespeichert. Das beeinträchtigt die Performance und führt zu Datenverlust.

Aktivieren Sie die Option nur im Ausnahmefall, wenn eine Korrektur der fehlerhaften Daten vor der Synchronisation nicht möglich ist.

Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus)

Wenn ein Zielsystemkonnektor das Zielsystem zeitweilig nicht erreichen kann, können Sie den Offline-Modus für dieses Zielsystem aktivieren. Damit können Sie verhindern, dass zielsystemspezifische Prozesse in der Jobqueue eingefroren werden und später manuell reaktiviert werden müssen.

Ob der Offline-Modus für eine Zielsystemverbindung grundsätzlich verfügbar ist, wird am Basisobjekt des jeweiligen Synchronisationsprojekts festgelegt. Sobald ein Zielsystem tatsächlich nicht erreichbar ist, kann diese Zielsystemverbindungen über das Launchpad offline und anschließend wieder online geschaltet werden.

Im Offline-Modus werden alle dem Basisobjekt zugewiesenen Jobserver angehalten. Dazu gehören der Synchronisationsserver und alle an der Lastverteilung beteiligten Jobserver. Falls einer der Jobserver auch andere Aufgaben übernimmt, dann werden diese ebenfalls nicht verarbeitet.

Voraussetzungen

Der Offline-Modus kann nur unter bestimmten Voraussetzungen für ein Basisobjekt zugelassen werden.

- Der Synchronisationsserver wird für kein anderes Basisobjekt als Synchronisationsserver genutzt.
- Wenn dem Basisobjekt eine Serverfunktion zugewiesen ist, darf keiner der Jobserver mit dieser Serverfunktion eine andere Serverfunktion (beispielsweise Aktualisierungsserver) haben.
- Es muss ein dedizierter Synchronisationsserver eingerichtet sein, der ausschließlich die Jobqueue für dieses Basisobjekt verarbeitet. Gleiches gilt für alle Jobserver, die über die Serverfunktion ermittelt werden.

Um den Offline-Modus für ein Basisobjekt zuzulassen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Basisobjekte**.
3. Wählen Sie in der Dokumentenansicht das Basisobjekt und klicken Sie .
4. Aktivieren Sie **Offline-Modus verfügbar**.
5. Klicken Sie **OK**.
6. Speichern Sie die Änderungen.

WICHTIG: Um Dateninkonsistenzen zu vermeiden, sollten Offline-Phasen kurz gehalten werden.

Die Zahl der nachträglich zu verarbeitenden Prozesse ist abhängig vom Umfang der Änderungen in der One Identity Manager-Datenbank mit Auswirkungen auf das Zielsystem während der Offline-Phase. Um Datenkonsistenz zwischen One Identity Manager-Datenbank und Zielsystem herzustellen, müssen alle anstehenden Prozesse verarbeitet werden, bevor eine Synchronisation gestartet wird.

Nutzen Sie den Offline-Modus möglichst nur, um kurzzeitige Systemausfälle, beispielsweise Wartungsfenster, zu überbrücken.

Um ein Zielsystem als offline zu kennzeichnen

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie **Verwalten > Systemüberwachung > Zielsysteme als offline kennzeichnen**.
3. Klicken Sie **Starten**.

   Der Dialog **Offline-Systeme verwalten** wird geöffnet. Im Bereich **Basisobjekte** werden die Basisobjekte aller Zielsystemverbindungen angezeigt, für die der Offline-Modus zugelassen ist.
4. Wählen Sie das Basisobjekt, dessen Zielsystemverbindung nicht verfügbar ist.
5. Klicken Sie **Offline schalten**.
6. Bestätigen Sie die Sicherheitsabfrage mit **OK**.

Damit werden die dem Basisobjekt zugewiesenen Jobserver angehalten. Es werden keine Synchronisations- und Provisionierungsaufträge ausgeführt. In Job Queue Info wird angezeigt, wenn ein Jobserver offline geschaltet wurde und die entsprechenden Aufträge nicht verarbeitet werden.

Ausführliche Informationen zum Offline-Modus finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Synchronisation deaktivieren auf Seite 47

Managen von PAM Benutzerkonten und Personen

Zentraler Bestandteil des One Identity Manager ist die Abbildung von Personen mit ihren Stammdaten sowie den Berechtigungen, über die sie in verschiedenen Zielsystemen verfügen. Zu diesem Zweck können Informationen über Benutzerkonten und Berechtigungen aus den Zielsystemen in die One Identity Manager-Datenbank eingelesen und mit den Personen verbunden werden. Für jede Person kann damit ein Überblick über ihre Berechtigungen in allen angebundenen Zielsystemen gewonnen werden. Der One Identity Manager bietet die Möglichkeit Benutzerkonten und ihre Berechtigungen zu verwalten. Änderungen können in die Zielsysteme provisioniert werden. Die Personen werden so entsprechend ihrer Funktion mit den benötigten Berechtigungen in den angebundenen Zielsystemen versorgt. Regelmäßige Synchronisationsprozesse halten die Daten zwischen den Zielsystemen und der One Identity Manager-Datenbank konsistent.

Da die Anforderungen von Unternehmen zu Unternehmen unterschiedlich sind, bietet der One Identity Manager verschiedene Verfahren zur Versorgung einer Person mit den benötigten Benutzerkonten an. Der One Identity Manager unterstützt die folgenden Vorgehensweisen, um Personen und ihre Benutzerkonten zu verknüpfen:

- Personen erhalten ihre Benutzerkonten automatisch über Kontendefinitionen.

  Hat eine Person noch kein Benutzerkonto in einer Appliance, wird durch die Zuweisung der Kontendefinition an eine Person über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

  Wenn Sie Benutzerkonten über Kontendefinitionen verwalten, können Sie das Verhalten von Benutzerkonten beim Deaktivieren oder Löschen von Personen festlegen.
- Beim Einfügen eines Benutzerkontos wird automatisch eine vorhandene Person zugeordnet oder im Bedarfsfall eine neue Person erstellt. Dabei werden die Personenstammdaten anhand vorhandener Benutzerkontenstammdaten erzeugt. Dieser Mechanismus kann eingesetzt werden, wenn ein neues Benutzerkonto manuell oder durch eine Synchronisation erstellt wird. Dieses Vorgehen ist jedoch nicht das Standardverfahren für den One Identity Manager. Für die automatische Personenzuordnung definieren Sie Kriterien, anhand derer die Personen ermittelt werden sollen.

- Personen und Benutzerkonten können manuell erfasst und einander zugeordnet werden.

Ausführliche Informationen zu den Grundlagen zur Behandlung und Administration von Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Kontendefinitionen für PAM Benutzerkonten auf Seite 57
- Automatische Zuordnung von Personen zu PAM Benutzerkonten auf Seite 79
- Kontendefinitionen an verbundene PAM Benutzerkonten zuweisen auf Seite 84
- Unterstützte Typen von Benutzerkonten auf Seite 86
- Löschverzögerung für PAM Benutzerkonten festlegen auf Seite 92
- PAM Benutzerkonten auf Seite 132

Kontendefinitionen für PAM Benutzerkonten

Um Benutzerkonten automatisch an Personen zu vergeben, kennt der One Identity Manager Kontendefinitionen. Kontendefinitionen können für jedes Zielsystem erzeugt werden. Hat eine Person noch kein Benutzerkonto in einem Zielsystem, wird durch die Zuweisung der Kontendefinition an eine Person ein neues Benutzerkonto erzeugt.

Aus den Personenstammdaten resultieren die Daten für das Benutzerkonto im jeweiligen Zielsystem. Die Personen müssen ein zentrales Benutzerkonto besitzen. Über die primäre Zuordnung der Person zu einem Standort, einer Abteilung, einer Kostenstelle oder einer Geschäftsrolle und die Zuweisung der IT Betriebsdaten zu diesen Unternehmensstrukturen wird automatisch die Zuteilung der IT Betriebsdaten zum Benutzerkonto der Person geregelt. Die Verarbeitung erfolgt über Bildungsregeln. In der Standardinstallation sind vordefinierte Bildungsregeln zur Ermittlung der benötigten Daten für die Benutzerkonten enthalten. Bei Bedarf können Sie die Bildungsregeln kundenspezifisch anpassen.

Für eine Kontendefinition legen Sie Automatisierungsgrade für die Behandlung der Benutzerkonten fest. Der Automatisierungsgrad eines Benutzerkontos entscheidet über den Umfang der vererbten Eigenschaften der Person an das Benutzerkonto. So kann beispielsweise eine Person mehrere Benutzerkonten in einem Zielsystem besitzen:

- Standardbenutzerkonto, welches alle Eigenschaften über die Person erbt
- Administratives Benutzerkonto, das zwar mit der Person verbunden ist, aber keine Eigenschaften von der Person erben soll

Ausführliche Informationen zu den Grundlagen zu Kontendefinitionen, Automatisierungsgraden und zur Ermittlung der gültigen IT Betriebsdaten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

- Erstellen von Kontendefinitionen
- Konfigurieren der Automatisierungsgrade
- Erstellen der Abbildungsvorschriften für die IT Betriebsdaten
- Erfassen der IT Betriebsdaten
- Zuweisen der Kontendefinitionen an Personen und Zielsysteme

Detaillierte Informationen zum Thema

- Kontendefinitionen erstellen auf Seite 58
- Kontendefinitionen bearbeiten auf Seite 59
- Stammdaten von Kontendefinitionen auf Seite 59
- Automatisierungsgrade bearbeiten auf Seite 62
- Automatisierungsgrade erstellen auf Seite 63
- Stammdaten von Automatisierungsgraden auf Seite 64
- Abbildungsvorschriften für IT Betriebsdaten erstellen auf Seite 65
- IT Betriebsdaten erfassen auf Seite 67
- IT Betriebsdaten ändern auf Seite 68
- Zuweisen der Kontendefinitionen an Personen auf Seite 69
- Kontendefinitionen an PAM Appliances zuweisen auf Seite 75
- Kontendefinitionen löschen auf Seite 76

Kontendefinitionen erstellen

Um eine Kontendefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular erfassen Sie die Stammdaten der Kontendefinition.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von Kontendefinitionen auf Seite 59
- Kontendefinitionen bearbeiten auf Seite 59
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 64

Kontendefinitionen bearbeiten

Um eine Kontendefinition zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten der Kontendefinition.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von Kontendefinitionen auf Seite 59
- Kontendefinitionen erstellen auf Seite 58
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 64

Stammdaten von Kontendefinitionen

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 7: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet. Für PAM Benutzer wählen Sie **PAGUser**.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte Kontendefinition	Angabe der vorausgesetzten Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch zugeordnet. Für eine PAM Appliance können Sie optional eine Active Directory Kontendefinition oder eine LDAP Kontendefinition wählen. In diesem Fall wird für die Person zunächst ein Active Directory oder LDAP Benutzerkonto erzeugt. Ist dieses Benutzerkonto vorhanden, wird das PAM Benutzerkonto als Verzeichnisbenutzer erstellt.

Eigenschaft	Beschreibung
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatisierungsgrad (initial)	Standardautomatisierungsgrad, der bei Neuanlage von Benutzerkonten standardmäßig verwendet werden soll.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Kontendefinition an Personen. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Leistungsposition	Leistungsposition, über welche die Kontendefinition im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.
IT Shop	Gibt an, ob die Kontendefinition über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Personen und Rollen außerhalb des IT Shop zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig.
Automatische Zuweisung zu Personen	Gibt an, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Um die Kontendefinition automatisch an alle internen Personen zuzuweisen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Personen aktivieren**. Die Kontendefinition wird an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine neue interne Person erstellt wird, erhält diese Person ebenfalls automatisch diese Kontendefinition. Um die automatische Zuweisung der Kontendefinition von allen Personen zu entfernen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Personen deaktivieren**. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.
Kontendefinition bei	Angabe zur Zuweisung der Kontendefinition an dauerhaft

Eigenschaft	Beschreibung
dauerhafter Deaktivierung beibehalten	deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei zeitweiliger Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei verzögertem Löschen beibehalten	Angabe zur Zuweisung der Kontendefinition bei verzögertem Löschen von Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei Sicherheitsgefährdung beibehalten	Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Ressourcentyp	Ressourcentyp zur Gruppierung von Kontendefinitionen.
Freies Feld 01- Freies Feld 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Gruppen erbbar	Gibt an, ob das Benutzerkonto Gruppen über die verbundene Person erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Person Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Person mit Benutzerkonto beispielsweise

Eigenschaft	Beschreibung
	in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Person eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Gruppe nur, wenn die Option aktiviert ist.

Automatisierungsgrade bearbeiten

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

- **Unmanaged**: Benutzerkonten mit dem Automatisierungsgrad **Unmanaged** erhalten eine Verbindung zur Person, erben jedoch keine weiteren Eigenschaften. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Person werden initial einige der Personeneigenschaften übernommen. Werden die Personeneigenschaften zu einem späteren Zeitpunkt geändert, dann werden diese Änderungen nicht an das Benutzerkonto weitergereicht.
- **Full managed**: Benutzerkonten mit dem Automatisierungsgrad **Full managed** erben definierte Eigenschaften der zugeordneten Person. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Person werden initial die Personeneigenschaften übernommen. Werden die Personeneigenschaften zu einem späteren Zeitpunkt geändert, dann werden diese Änderungen an das Benutzerkonto weitergereicht.

HINWEIS: Die Automatisierungsgrade **Full managed** und **Unmanaged** werden in Bildungsregeln ausgewertet. Die mitgelieferten Bildungsregeln können Sie im Designer unternehmensspezifisch anpassen.

Abhängig von Ihren Anforderungen können Sie weitere Automatisierungsgrade definieren. Die Bildungsregeln müssen Sie um die Vorgehensweise für die zusätzlichen Automatisierungsgrade erweitern.

Legen Sie für jeden Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll. Ausführliche Informationen zu Automatisierungsgraden finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

- Um die Berechtigungen zu entziehen, wenn eine Person deaktiviert, gelöscht oder als sicherheitsgefährdend eingestuft wird, können die Benutzerkonten der Person gesperrt werden. Wird die Person zu einem späteren Zeitpunkt wieder aktiviert, werden ihre Benutzerkonten ebenfalls wieder freigeschaltet.

- Zusätzlich kann die Vererbung der Gruppenmitgliedschaften definiert werden. Die Unterbrechung der Vererbung kann beispielsweise gewünscht sein, wenn die Benutzerkonten einer Person gesperrt sind und somit auch nicht in Gruppen Mitglied sein dürfen. Während dieser Zeit sollen keine Vererbungsvorgänge für diese Personen berechnet werden. Bestehende Gruppenmitgliedschaften werden dann gelöscht!

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Automatisierungsgrades.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von Automatisierungsgraden auf Seite 64
- Automatisierungsgrade erstellen auf Seite 63
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 64

Automatisierungsgrade erstellen

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade **Unmanaged** und **Full managed**. Abhängig von Ihren Anforderungen können Sie weitere Automatisierungsgrade definieren.

WICHTIG: Erweitern Sie im Designer die Bildungsregeln um die Vorgehensweise für die zusätzlichen Automatisierungsgrade. Ausführliche Informationen zu Bildungsregeln finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um einen Automatisierungsgrad zu erstellen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Automatisierungsgrade**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten des Automatisierungsgrades.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von Automatisierungsgraden auf Seite 64
- Automatisierungsgrade bearbeiten auf Seite 62
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 64

Automatisierungsgrade an Kontendefinitionen zuweisen

WICHTIG: Der Automatisierungsgrad **Unmanaged** wird beim Erstellen einer Kontendefinition automatisch zugewiesen und kann nicht entfernt werden.

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Automatisierungsgrade zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Automatisierungsgrade zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Automatisierungsgrad und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Stammdaten von Automatisierungsgraden

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 8: Stammdaten eines Automatisierungsgrades

Eigenschaft	Beschreibung
Automatisierungsgrad	Bezeichnung des Automatisierungsgrades.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Betriebsdaten überschreibend	Gibt an, ob Daten an Benutzerkonten, die sich aus den IT Betriebsdaten bilden, automatisch aktualisiert werden. Zulässige Werte sind: • **Niemals**: Die Daten werden nicht aktualisiert.

Eigenschaft	Beschreibung
	(Standard) • **Immer**: Die Daten werden immer aktualisiert. • **Nur initial**: Die Daten werden nur initial ermittelt.
Gruppen bei zeitweiliger Deaktivierung beibehalten	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei zeitweiliger Deaktivierung sperren	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Personen gesperrt werden sollen.
Gruppen bei dauerhafter Deaktivierung beibehalten	Gibt an, ob die Benutzerkonten dauerhaft deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei dauerhafter Deaktivierung sperren	Gibt an, ob die Benutzerkonten dauerhaft deaktivierter Personen gesperrt werden sollen.
Gruppen bei verzögertem Löschen beibehalten	Gibt an, ob die Benutzerkonten zum Löschen markierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei verzögertem Löschen sperren	Gibt an, ob die Benutzerkonten zum Löschen markierter Personen gesperrt werden sollen.
Gruppen bei Sicherheitsgefährdung beibehalten	Gibt an, ob die Benutzerkonten von sicherheitsgefährdenden Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei Sicherheitsgefährdung sperren	Gibt an, ob die Benutzerkonten von sicherheitsgefährdenden Personen gesperrt werden sollen.
Gruppen bei deaktiviertem Benutzerkonto beibehalten	Gibt an, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen.

Abbildungsvorschriften für IT Betriebsdaten erstellen

Eine Kontendefinition legt fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über die primären Rollen einer Person ermittelt werden können.

Die folgenden IT Betriebsdaten werden in der Standardkonfiguration des One Identity Manager für das automatische Erzeugen und Ändern von Benutzerkonten für eine Person im Zielsystem verwendet.

- PAM Authentifizierungsanbieter
- PAM Identitätsanbieter
- PAM Sekundäre Authentifizierung
- PAM Administrative Berechtigungen
- Gruppen erbbar
- Identität
- Privilegiertes Benutzerkonto

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **IT Betriebsdaten Abbildungsvorschrift bearbeiten.**
4. Klicken Sie **Hinzufügen** und erfassen Sie folgende Informationen.
    - **Spalte**: Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.
    - **Quelle**: Angabe, welche Rolle verwendet wird, um die Eigenschaften für das Benutzerkonto zu ermitteln. Zur Auswahl stehen:
        - Primäre Abteilung
        - Primärer Standort
        - Primäre Kostenstelle
        - Primäre Geschäftsrolle

          HINWEIS: Die Geschäftsrolle kann nur verwendet werden, wenn das Geschäftsrollenmodul vorhanden ist.
        - keine Angabe

          Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option **Immer Standardwert verwenden** setzen.
    - **Standardwert**: Standardwert der Eigenschaft für das Benutzerkonto einer Person, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann.
    - **Immer Standardwert verwenden**: Gibt an, ob die Eigenschaft des Benutzerkontos immer mit dem Standardwert besetzt wird. Es erfolgt keine dynamische Ermittlung der IT Betriebsdaten aus einer Rolle.

- **Benachrichtigung bei Verwendung des Standards**: Gibt an, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkontos mit Standardwerten** verwendet.

  Um die Mailvorlage zu ändern, passen Sie im Designer den Konfigurationsparameter **TargetSystem | PAG | Accounts | MailTemplateDefaultValues** an.

5. Speichern Sie die Änderungen.

Verwandte Themen

- IT Betriebsdaten erfassen auf Seite 67
- IT Betriebsdaten ändern auf Seite 68

IT Betriebsdaten erfassen

Um für eine Person Benutzerkonten mit dem Automatisierungsgrad **Full managed** zu erzeugen, müssen die benötigten IT Betriebsdaten ermittelt werden. Welche IT Betriebsdaten für welches Zielsystem konkret verwendet werden sollen, wird an den Geschäftsrollen, Abteilungen, Kostenstellen oder Standorten definiert. Einer Person wird eine primäre Geschäftsrolle, eine primäre Abteilung, eine primäre Kostenstelle oder ein primärer Standort zugeordnet. Abhängig von dieser Zuordnung werden die gültigen IT Betriebsdaten ermittelt und für die Erstellung des Benutzerkontos verwendet. Können über die primären Rollen keine gültigen IT Betriebsdaten ermittelt werden, werden die Standardwerte verwendet.

Wenn in einem Zielsystem mehrere Kontendefinitionen für die Abbildung der Benutzerkonten verwendet werden, können Sie die IT Betriebsdaten auch direkt für eine konkrete Kontendefinition festlegen.

Beispiel:

In der Regel erhält jede Person der Abteilung A ein Standardbenutzerkonto in der Appliance A. Zusätzlich erhalten einige Personen der Abteilung A administrative Benutzerkonten in der Appliance A.

Erstellen Sie eine Kontendefinition A für die Standardbenutzerkonten der Appliance A und eine Kontendefinition B für die administrativen Benutzerkonten der Appliance A. In der Abbildungsvorschrift der IT Betriebsdaten für die Kontendefinitionen A und B legen Sie die Eigenschaft **Abteilung** zur Ermittlung der gültigen IT Betriebsdaten fest.

Für die Abteilung A legen Sie die wirksamen IT Betriebsdaten für die Appliance A fest. Diese IT Betriebsdaten werden für die Standardbenutzerkonten verwendet.

Zusätzlich legen Sie für die Abteilung A die wirksamen IT Betriebsdaten für die Kontendefinition B fest. Diese IT Betriebsdaten werden für administrative Benutzerkonten verwendet.

Um IT Betriebsdaten festzulegen

1. Wählen Sie im Manager in der Kategorie **Organisationen** oder **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten**.
3. Klicken Sie **Hinzufügen** und erfassen Sie die folgenden Daten.
   - **Wirksam für**: Legen Sie den Anwendungsbereich der IT Betriebsdaten fest. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden.

     Um den Anwendungsbereich festzulegen

     a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.

     b. Wählen Sie unter **Tabelle** die Tabelle, die das Zielsystem abbildet oder, für eine Kontendefinition, die Tabelle `TSBAccountDef`.

     c. Wählen Sie unter **Wirksam für** das konkrete Zielsystem oder die konkrete Kontendefinition.

     d. Klicken Sie **OK**.
   - **Spalte**: Wählen Sie die Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird.

     In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.
   - **Wert**: Erfassen Sie den konkreten Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Abbildungsvorschriften für IT Betriebsdaten erstellen auf Seite 65
- IT Betriebsdaten ändern auf Seite 68

IT Betriebsdaten ändern

Sobald sich die IT Betriebsdaten ändern, müssen Sie diese Änderungen für bestehende Benutzerkonten übernehmen. Dafür führen Sie die Bildungsregeln an den betroffenen Spalten erneut aus. Bevor Sie die Bildungsregeln ausführen, prüfen Sie, welche

Auswirkungen eine Änderung der IT Betriebsdaten auf bestehende Benutzerkonten hat. Für jede betroffene Spalte an jedem betroffenen Benutzerkonto können Sie entscheiden, ob die Änderung in die One Identity Manager-Datenbank übernommen werden soll.

Voraussetzungen

- Die IT Betriebsdaten einer Abteilung, einer Kostenstelle, einer Geschäftsrolle oder eines Standorts wurden geändert.

  - ODER -

- Die Standardwerte in der IT Betriebsdaten Abbildungsvorschrift für eine Kontendefinition wurden geändert.

HINWEIS: Ändert sich die Zuordnung einer Person zu einer primären Abteilung, Kostenstelle, zu einer primären Geschäftsrolle oder zu einem primären Standort, werden die Bildungsregeln automatisch ausgeführt.

Um die Bildungsregeln auszuführen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Bildungsregeln ausführen**.

   Es wird eine Liste aller Benutzerkonten angezeigt, die über die gewählte Kontendefinition entstanden sind und deren Eigenschaften durch die Änderung der IT Betriebsdaten geändert werden. Es bedeuten:

   - **Alter Wert**: Wert der Objekteigenschaft vor der Änderung der IT Betriebsdaten.
   - **Neuer Wert**: Wert der Objekteigenschaft nach der Änderung der IT Betriebsdaten.
   - **Auswahl**: Gibt an, ob der neue Wert für das Benutzerkonto übernommen werden soll.
4. Markieren Sie in der Spalte **Auswahl** alle Objekteigenschaften, für die der neue Wert übernommen werden soll.
5. Klicken Sie **Übernehmen**.

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinitionen an Personen

Kontendefinitionen werden an die Personen des Unternehmens zugewiesen.

Das Standardverfahren für die Zuweisung von Kontendefinitionen an Personen ist die indirekte Zuweisung. Die Kontendefinitionen werden an die Abteilungen, Kostenstellen,

Standorte oder Geschäftsrollen zugewiesen. Die Personen werden gemäß ihrer Funktion im Unternehmen in diese Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen eingeordnet und erhalten so ihre Kontendefinitionen. Um auf Sonderanforderungen zu reagieren, können einzelne Kontendefinitionen direkt an Personen zugewiesen werden.

Kontendefinitionen können automatisch an alle Personen eines Unternehmens zugewiesen werden. Es ist möglich, die Kontendefinitionen als bestellbare Produkte dem IT Shop zuzuordnen. Der Abteilungsleiter kann dann für seine Mitarbeiter Benutzerkonten über das Web Portal bestellen. Zusätzlich ist es möglich, Kontendefinitionen in Systemrollen aufzunehmen. Diese Systemrollen können über hierarchische Rollen oder direkt an Personen zugewiesen werden oder als Produkte in den IT Shop aufgenommen werden.

In den Prozessen der One Identity Manager Standardinstallation wird zunächst überprüft, ob die Person bereits ein Benutzerkonto im Zielsystem der Kontendefinition besitzt. Ist kein Benutzerkonto vorhanden, so wird ein neues Benutzerkonto mit dem Standardautomatisierungsgrad der zugewiesenen Kontendefinition erzeugt.

HINWEIS: Ist bereits ein Benutzerkonto vorhanden und ist es deaktiviert, dann wird dieses Benutzerkonto entsperrt. Den Automatisierungsgrad des Benutzerkontos müssen Sie in diesem Fall nachträglich ändern.

HINWEIS: Solange eine Kontendefinition für eine Person wirksam ist, behält die Person ihr daraus entstandenes Benutzerkonto. Wird die Zuweisung einer Kontendefinition entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht.

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

- Für die Rollenklasse (Abteilung, Kostenstelle, Standort oder Geschäftsrolle) ist die Zuweisung von Personen und Kontendefinitionen erlaubt.

Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

1. Wählen Sie im Manager in der Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.

   - ODER -

   Wählen Sie im Manager in der Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.
2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
   - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
   - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
3. Speichern Sie die Änderungen.

Ausführliche Informationen zur Vorbereitung der Rollenklassen für die Zuweisung finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Detaillierte Informationen zum Thema

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 71
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 71
- Kontendefinitionen an alle Personen zuweisen auf Seite 72
- Kontendefinitionen direkt an Personen zuweisen auf Seite 72
- Kontendefinitionen an Systemrollen zuweisen auf Seite 73
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 73

Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
    - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
    - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
    - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

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

    Um eine Zuweisung zu entfernen

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

Kontendefinitionen an Geschäftsrollen zuweisen

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

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.

3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Kontendefinitionen an alle Personen zuweisen

Über diese Aufgaben wird die Kontendefinition an alle internen Personen zugewiesen. Personen, die als externe Personen gekennzeichnet sind, erhalten die Kontendefinition nicht. Sobald eine neue interne Person erstellt wird, erhält diese Person ebenfalls automatisch diese Kontendefinition. Die Zuweisung wird durch den DBQueue Prozessor berechnet.

WICHTIG: Führen Sie die Aufgabe nur aus, wenn sichergestellt ist, dass alle aktuell in der Datenbank vorhandenen internen Personen sowie alle zukünftig neu hinzuzufügenden internen Personen ein Benutzerkonto in diesem Zielsystem erhalten sollen!

Um eine Kontendefinition an alle Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Automatische Zuweisung zu Personen aktivieren**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Speichern Sie die Änderungen.

HINWEIS: Um die automatische Zuweisung der Kontendefinition von allen Personen zu entfernen, führen Sie die Aufgabe **Automatische Zuweisung zu Personen deaktivieren** aus. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen bleiben jedoch erhalten.

Kontendefinitionen direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.

3. Wählen Sie die Aufgabe **An Personen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

   Um eine Zuweisung zu entfernen

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

Kontendefinitionen an Systemrollen zuweisen

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

Kontendefinitionen, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können Sie nur an Systemrollen zuweisen, bei denen diese Option ebenfalls aktiviert ist.

Um Kontendefinitionen in eine Systemrolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Kontendefinitionen in den IT Shop aufnehmen

Mit der Zuweisung einer Kontendefinition an ein IT Shop Regal kann sie von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Die Kontendefinition muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Kontendefinition muss eine Leistungsposition zugeordnet sein.

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Kontendefinition im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.

- Soll die Kontendefinition nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss sie zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen ist dann nicht mehr zulässig.

HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren Kontendefinitionen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Kontendefinition in den IT Shop aufzunehmen.

Um eine Kontendefinition in den IT Shop aufzunehmen (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontendefinition an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Kontendefinition in den IT Shop aufzunehmen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontendefinition an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Kontendefinition aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.

3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Kontendefinition aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.

Ausführliche Informationen zur Bestellung von Unternehmensressourcen über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Verwandte Themen

- Stammdaten von Kontendefinitionen auf Seite 59

Kontendefinitionen an PAM Appliances zuweisen

Wenn Sie die automatische Zuordnung von Benutzerkonten und Personen einsetzen und dabei bereits verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen sollen, sind folgende Voraussetzungen zu gewährleisten:

- Die Kontendefinition ist dem Zielsystem zugewiesen.
- Die Kontendefinition besitzt einen Standardautomatisierungsgrad.

Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen Synchronisation der Fall.

Um die Kontendefinition an ein Zielsystem zuzuweisen

1. Wählen Sie im Manager in der Kategorie **Privileged Account Management > Appliances** die Appliance.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie in der Auswahlliste **Kontendefinition (initial)** die Kontendefinition für die Benutzerkonten.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Automatische Zuordnung von Personen zu PAM Benutzerkonten auf Seite 79

Kontendefinitionen löschen

Sie können Kontendefinitionen löschen, wenn diese keinem Zielsystem, keiner Person, keiner hierarchischen Rolle und keiner anderen Kontendefinition als Vorgänger zugeordnet sind.

Um eine Kontendefinition zu löschen

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Personen.
    a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Wählen Sie die Aufgabe **Automatische Zuweisung zu Personen deaktivieren**.
    e. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
    f. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Personen.
    a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

c. Wählen Sie die Aufgabe **An Personen zuweisen**.

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

e. Speichern Sie die Änderungen.

3. Entfernen Sie die Zuordnung der Kontendefinition zu Abteilungen, Kostenstellen und Standorten.

   a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

   c. Wählen Sie die Aufgabe **Organisationen zuweisen**.

   d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Abteilungen, Kostenstellen und Standorte.

   e. Speichern Sie die Änderungen.

4. Entfernen Sie die Zuordnung der Kontendefinition zu Geschäftsrollen.

   a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

   c. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.

   d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.

   e. Speichern Sie die Änderungen.

5. Wenn die Kontendefinition über den IT Shop bestellt wurde, muss sie abbestellt und aus allen IT Shop Regalen entfernt werden.

   Ausführliche Informationen zum Abbestellen einer Bestellung finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.

   Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen (bei rollenbasierter Anmeldung)

   a. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

   c. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.

   d. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   e. Klicken Sie **OK**.

      Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen (bei nicht-rollenbasierter Anmeldung)

a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

c. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.

d. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

e. Klicken Sie **OK**.

Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.

6. Entfernen Sie die Zuordnung der Kontendefinition als vorausgesetzte Kontendefinition einer anderen Kontendefinition. Solange die Kontendefinition Voraussetzung einer anderen Kontendefinition ist, kann sie nicht gelöscht werden. Prüfen Sie alle Kontendefinitionen.

   a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

   d. Entfernen Sie in der Auswahlliste **Vorausgesetzte Kontendefinition** die Kontendefinition.

   e. Speichern Sie die Änderungen.

7. Entfernen Sie die Zuordnung der Kontendefinition zum Zielsystem.

   a. Wählen Sie im Manager in der Kategorie **Privileged Account Management > Appliances** die Appliance.

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

   c. Entfernen Sie auf dem Tabreiter **Allgemein** die zugewiesenen Kontendefinitionen.

   d. Speichern Sie die Änderungen.

8. Löschen Sie die Kontendefinition.

   a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

   c. Klicken Sie , um die Kontendefinition zu löschen.

Automatische Zuordnung von Personen zu PAM Benutzerkonten

Beim Einfügen eines Benutzerkontos kann automatisch eine vorhandene Person zugeordnet werden. Im Bedarfsfall kann eine Person neu erstellt werden. Dabei werden die Personenstammdaten anhand vorhandener Benutzerstammdaten erzeugt. Dieser Mechanismus kann auf die Erstellung eines neuen Benutzerkontos durch manuelle Anlage oder Synchronisation folgen.

Für die automatische Personenzuordnung definieren Sie Kriterien für die Ermittlung der Personen. Wird durch den eingesetzten Modus ein Benutzerkonto mit einer Person verbunden, so erhält das Benutzerkonto durch interne Verarbeitung den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Abhängig davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden.

Schalten Sie das Verfahren im laufenden Betrieb ein, erfolgt ab diesem Zeitpunkt die automatische Zuordnung der Personen zu Benutzerkonten. Deaktivieren Sie das Verfahren zu einem späteren Zeitpunkt wieder, wirkt sich diese Änderung nur auf Benutzerkonten aus, die ab diesem Zeitpunkt angelegt oder aktualisiert werden. Bereits vorhandene Zuordnungen von Personen zu Benutzerkonten bleiben bestehen.

> HINWEIS: Für administrative Benutzerkonten wird empfohlen, die Zuordnung der Personen nicht über die automatische Personenzuordnung vorzunehmen. Ordnen Sie Personen zu administrativen Benutzerkonten über die Aufgabe **Stammdaten bearbeiten** am jeweiligen Benutzerkonto zu.

Ausführliche Informationen zur automatischen Personenzuordnung finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Führen Sie folgende Aktionen aus, damit Personen automatisch zugeordnet werden können.

- Wenn Personen bei der Synchronisation von Benutzerkonten zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | PAG | PersonAutoFullsync** und wählen Sie den gewünschte Modus.
- Wenn Personen außerhalb der Synchronisation zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | PAG | PersonAutoDefault** und wählen Sie den gewünschten Modus.
- Legen Sie im Konfigurationsparameter **TargetSystem | PAG | PersonExcludeList** die Benutzerkonten fest, für die keine automatische Zuordnung zu Personen erfolgen soll.

  Beispiel:

  ```
  ADMINISTRATOR|GUEST
  ```

  > TIPP: Den Wert des Konfigurationsparameters können Sie über den Dialog **Ausschlussliste für die automatische Personenzuordnung** bearbeiten.

Um die Ausschlussliste für die automatische Personenzuordnung zu bearbeiten

1. Bearbeiten Sie im Designer den Konfigurationsparameter **PersonExcludeList**.
2. Klicken Sie **...** hinter dem Eingabefeld **Wert**.

   Der Dialog **Ausschlussliste für PAM Benutzerkonten** wird geöffnet.
3. Um einen neuen Eintrag einzufügen, klicken Sie **Neu**.

   Um einen Eintrag zu bearbeiten, wählen Sie den Eintrag und klicken Sie **Bearbeiten**.
4. Erfassen Sie die Bezeichnung des Benutzerkontos, dem Personen nicht automatisch zugeordnet werden sollen.

   Jeder Eintrag in der Liste wird als Teil eines regulären Ausdrucks behandelt. Metazeichen für reguläre Ausdrücke können verwendet werden.
5. Um einen Eintrag zu löschen, wählen Sie den Eintrag und klicken Sie **Löschen**.
6. Klicken Sie **OK**.

- Legen Sie über den Konfigurationsparameter **TargetSystem | PAG | PersonAutoDisabledAccounts** fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
- Weisen Sie der Appliance eine Kontendefinition zu. Stellen Sie sicher, dass der Automatisierungsgrad, der verwendet werden soll, als Standardautomatisierungsgrad eingetragen ist.
- Definieren Sie die Suchkriterien für die Personenzuordnung an dieser Appliance.

HINWEIS:

Für die Synchronisation gilt:

- Die automatische Personenzuordnung wirkt, wenn Benutzerkonten neu angelegt oder aktualisiert werden.

Außerhalb der Synchronisation gilt:

- Die automatische Personenzuordnung wirkt, wenn Benutzerkonten neu angelegt werden.

HINWEIS:

Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Personen erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für die Appliance bekannt, werden die Benutzerkonten mit den Personen verbunden. Es wird jedoch noch keine Kontendefinition zugewiesen. Die Benutzerkonten sind somit im Zustand **Linked** (verbunden).

Um die Benutzerkonten über Kontendefinitionen zu verwalten, weisen Sie diesen Benutzerkonten eine Kontendefinition und einen Automatisierungsgrad zu.

Weitere Informationen finden Sie unter PAM Benutzerkonten über Kontendefinitionen verwalten auf Seite 51.

Verwandte Themen

- Kontendefinitionen erstellen auf Seite 58
- Kontendefinitionen an PAM Appliances zuweisen auf Seite 75
- Automatisierungsgrade für PAM Benutzerkonten ändern auf Seite 84
- Kontendefinitionen an verbundene PAM Benutzerkonten zuweisen auf Seite 84
- Suchkriterien für die automatische Personenzuordnung bearbeiten auf Seite 81

Suchkriterien für die automatische Personenzuordnung bearbeiten

HINWEIS: Der One Identity Manager liefert ein Standardmapping für die Personenzuordnung. Führen Sie die folgenden Schritte nur aus, wenn Sie das Standardmapping unternehmensspezifisch anpassen möchten.

Die Kriterien für die Personenzuordnung werden an der Appliance definiert. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person dem Benutzerkonto zugeordnet werden kann. Die Suchkriterien können Sie durch Formatdefinitionen weiter einschränken.

Das zusammengestellte Suchkriterium wird in XML-Notation in die Spalte **Suchkriterien für die automatische Personenzuordnung** (`AccountToPersonMatchingRule`) der Tabelle `PAGUser` geschrieben.

Die Suchkriterien werden bei der automatischen Zuordnung von Personen zu Benutzerkonten ausgewertet. Darüber hinaus können Sie anhand der Suchkriterien eine Vorschlagsliste für die Personenzuordnung an Benutzerkonten erzeugen und die Zuordnung direkt ausführen.

HINWEIS: Die Objektdefinitionen für Benutzerkonten, auf welche die Suchkriterien angewendet werden können, sind vordefiniert. Sollten Sie weitere Objektdefinitionen benötigen, um beispielsweise die Vorauswahl der Benutzerkonten weiter einzuschränken, erzeugen Sie im Designer die entsprechenden kundenspezifische Objektdefinitionen. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um Kriterien für die Personenzuordnung festzulegen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances**.
2. Wählen Sie in der Ergebnisliste die Appliance.
3. Wählen Sie die Aufgabe **Suchkriterien für die Personenzuordnung definieren**.
4. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person mit dem

Benutzerkonto verbunden wird.

Tabelle 9: Standardsuchkriterien für Benutzerkonten

Anwenden auf	Spalte an Person	Spalte am Benutzerkonto
PAM Benutzerkonten (Lokale Benutzer)	Zentrales Benutzerkonto (`CentralAccount`)	Benutzername (`UserName`)

5. Speichern Sie die Änderungen.

Ausführliche Informationen zur Definition der Suchkriterien finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Automatische Zuordnung von Personen zu PAM Benutzerkonten auf Seite 79
- Personen suchen und direkt an Benutzerkonten zuordnen auf Seite 82

Personen suchen und direkt an Benutzerkonten zuordnen

Anhand der Suchkriterien können Sie eine Vorschlagsliste für die Personenzuordnung an Benutzerkonten erzeugen und die Zuordnung direkt ausführen. Die Benutzerkonten sind dafür in verschiedenen Ansichten zusammengestellt.

Tabelle 10: Ansichten zur manuellen Zuordnung

Ansicht	Beschreibung
Vorgeschlagene Zuordnungen	Die Ansicht listet alle Benutzerkonten auf, denen der One Identity Manager eine Person zuordnen kann. Dazu werden die Personen angezeigt, die durch die Suchkriterien ermittelt und zugeordnet werden können.
Zugeordnete Benutzerkonten	Die Ansicht listet alle Benutzerkonten auf, denen eine Person zugeordnet ist.
Ohne Personenzuordnung	Die Ansicht listet alle Benutzerkonten auf, denen keine Person zugeordnet ist und für die über die Suchkriterien keine passende Person ermittelt werden kann.

Um Suchkriterien auf die Benutzerkonten anzuwenden

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances**.

2. Wählen Sie in der Ergebnisliste die Appliance.
3. Wählen Sie die Aufgabe **Suchkriterien für die Personenzuordnung definieren**.
4. Im unteren Bereich des Formulars klicken Sie **Neu laden**.

   Für alle Benutzerkonten im Zielsystem werden die möglichen Zuordnungen anhand der Suchkriterien ermittelt. Die drei Ansichten werden aktualisiert.

TIPP: Mit Maus-Doppelklick auf einen Eintrag in den Ansichten werden das Benutzerkonto und die Person geöffnet und Sie können die Stammdaten einsehen.

Durch die Zuordnung von Personen an die Benutzerkonten entstehen verbundene Benutzerkonten (Zustand **Linked**). Um verwaltete Benutzerkonten zu erhalten (Zustand **Linked configured**), können Sie gleichzeitig eine Kontendefinition zuordnen.

Um Personen direkt über die Vorschlagsliste zuzuordnen

- Klicken Sie **Vorgeschlagene Zuordnungen**.
  1. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die vorgeschlagene Person zugeordnet werden soll. Eine Mehrfachauswahl ist möglich.
  2. (Optional) Wählen Sie im Auswahlfeld **Diese Kontendefinition zuweisen** eine Kontendefinition und im Auswahlfeld **Diesen Automatisierungsgrad zuweisen** einen Automatisierungsgrad.
  3. Klicken Sie **Ausgewählte zuweisen.**
  4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

     Den ausgewählten Benutzerkonten werden die per Suchkriterium ermittelten Personen zugeordnet. Wenn eine Kontendefinition ausgewählt wurde, wird diese an alle ausgewählten Benutzerkonten zugeordnet.

  - ODER -

- Klicken Sie **Ohne Personenzuordnung**.
  1. Klicken Sie **Person auswählen** für das Benutzerkonto, dem eine Person zugeordnet werden soll. Wählen Sie eine Person aus der Auswahlliste.
  2. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die ausgewählten Personen zugeordnet werden sollen. Eine Mehrfachauswahl ist möglich.
  3. (Optional) Wählen Sie im Auswahlfeld **Diese Kontendefinition zuweisen** eine Kontendefinition und im Auswahlfeld **Diesen Automatisierungsgrad zuweisen** einen Automatisierungsgrad.
  4. Klicken Sie **Ausgewählte zuweisen**.
  5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

     Den ausgewählten Benutzerkonten werden die Personen zugeordnet, die in der Spalte **Person** angezeigt werden. Wenn eine Kontendefinition ausgewählt wurde, wird diese an alle ausgewählten Benutzerkonten zugeordnet.

Um Zuordnungen zu entfernen

- Klicken Sie **Zugeordnete Benutzerkonten**.
    1. Klicken Sie **Auswahl** für alle Benutzerkonten, deren Personenzuordnung entfernt werden soll. Mehrfachauswahl ist möglich.
    2. Klicken Sie **Ausgewählte entfernen**.
    3. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

       Von den ausgewählten Benutzerkonten werden die zugeordneten Personen entfernt.

Automatisierungsgrade für PAM Benutzerkonten ändern

Wenn Sie Benutzerkonten über die automatische Personenzuordnung erstellen, wird der Standardautomatisierungsgrad genutzt. Sie können den Automatisierungsgrad eines Benutzerkontos nachträglich ändern.

Um den Automatisierungsgrad für ein Benutzerkonto zu ändern

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Automatisierungsgrad** den Automatisierungsgrad.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für PAM Benutzerkonten auf Seite 138

Kontendefinitionen an verbundene PAM Benutzerkonten zuweisen

An Benutzerkonten im Zustand **Linked** (verbunden) kann nachträglich eine Kontendefinition zugewiesen werden. Das kann beispielsweise der Fall sein, wenn

- Personen und Benutzerkonten manuell verbunden wurden
- die automatische Personenzuordnung konfiguriert ist, beim Einfügen eines Benutzerkontos jedoch noch keine Kontendefinition an die Appliance zugeordnet ist

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie der Appliance die Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand **Linked** (verbunden) die Kontendefinition zu. Es wird der Standardautomatisierungsgrad der Kontendefinition für das Benutzerkonto übernommen.
    a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten > Verbunden aber nicht konfiguriert > <Appliance>**.
    b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.
    c. Wählen Sie in der Auswahlliste **Kontendefinition** die Kontendefinition.
    d. Wählen Sie die Benutzerkonten, die die Kontendefinition erhalten sollen.
    e. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Kontendefinitionen an PAM Appliances zuweisen auf Seite 75

Personen manuell mit PAM Benutzerkonten verbinden

Eine Person kann mit mehreren PAM Benutzerkonten verbunden werden, beispielsweise um zusätzlich zum Standardbenutzerkonto ein administratives Benutzerkonto zuzuweisen. Darüber hinaus kann eine Person Standardbenutzerkonten mit verschiedenen Typen nutzen.

HINWEIS: Um mit Identitäten für Benutzerkonten zu arbeiten, benötigen die Personen ebenfalls Identitäten. Benutzerkonten, denen eine Identität zugeordnet ist, können Sie nur mit Personen verbinden, die dieselbe Identität haben.

Um einer Person manuell Benutzerkonten zuzuweisen

1. Wählen Sie im Manager die Kategorie **Personen | Personen**.
2. Wählen Sie in der Ergebnisliste die Person und führen Sie die Aufgabe **PAM Benutzerkonten zuweisen** aus.
3. Weisen Sie die Benutzerkonten zu.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Unterstützte Typen von Benutzerkonten auf Seite 86

Unterstützte Typen von Benutzerkonten

Im One Identity Manager können unterschiedliche Typen von Benutzerkonten wie beispielsweise Standardbenutzerkonten, administrative Benutzerkonten, Dienstkonten oder privilegierte Benutzerkonten abgebildet werden.

Zur Abbildung der verschiedenen Benutzerkontentypen werden die folgenden Eigenschaften verwendet.

- Identität

  Mit der Eigenschaft **Identität** (Spalte `IdentityType`) wird der Typ des Benutzerkontos beschrieben.

  Tabelle 11: Identitäten von Benutzerkonten

Identität	Beschreibung	Wert der Spalte IdentityType
Primäre Identität	Standardbenutzerkonto einer Person.	Primary
Organisatorische Identität	Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen.	Organizational
Persönliche Administratoridentität	Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird.	Admin
Zusatzidentität	Benutzerkonto, das für einen spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken.	Sponsored
Gruppenidentität	Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird.	Shared
Dienstidentität	Dienstkonto.	Service

  HINWEIS: Um mit Identitäten für Benutzerkonten zu arbeiten, benötigen die Personen ebenfalls Identitäten. Benutzerkonten, denen eine Identität zugeordnet ist, können Sie nur mit Personen verbinden, die dieselbe Identität haben.

  Die primäre Identität, die organisatorische Identität und die persönliche Administratoridentität werden für die verschiedenen Benutzerkonten genutzt, mit denen ein und dieselbe Person ihre unterschiedlichen Aufgaben im Unternehmen ausführen kann.

Um Benutzerkonten mit einer persönlichen Administratoridentität oder einer organisatorischen Identität für eine Person bereitzustellen, richten Sie für die Person Subidentitäten ein. Diese Subidentitäten verbinden Sie mit den Benutzerkonten. Somit können für die unterschiedlichen Benutzerkonten die erforderlichen Berechtigungen erteilt werden.

Benutzerkonten mit einer Zusatzidentität, einer Gruppenidentität oder einer Dienstidentität verbinden Sie mit Pseudo-Personen, die keinen Bezug zu einer realen Person haben. Diese Pseudo-Personen werden benötigt, um Berechtigungen an die Benutzerkonten vererben zu können. Bei der Auswertung von Berichten, Attestierungen oder Complianceprüfungen prüfen Sie, ob die Pseudo-Personen gesondert betrachtet werden müssen.

Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

- Privilegiertes Benutzerkonto

  Privilegierte Benutzerkonten werden eingesetzt, um Personen mit zusätzlichen privilegierten Berechtigungen auszustatten. Dazu gehören beispielsweise administrative Benutzerkonten oder Dienstkonten. Die Benutzerkonten werden mit der Eigenschaft **Privilegiertes Benutzerkonto** (Spalte `IsPrivilegedAccount`) gekennzeichnet.

Detaillierte Informationen zum Thema

- Standardbenutzerkonten auf Seite 87
- Administrative Benutzerkonten auf Seite 88
- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 89
- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 90
- Privilegierte Benutzerkonten auf Seite 91

Standardbenutzerkonten

In der Regel erhält jede Person ein Standardbenutzerkonto, das die Berechtigungen besitzt, die für die tägliche Arbeit benötigt werden. Die Benutzerkonten haben eine Verbindung zur Person. Über eine Kontendefinition und deren Automatisierungsgrade kann die Auswirkung der Verbindung und der Umfang der vererbten Eigenschaften der Person an die Benutzerkonten konfiguriert werden.

Um Standardbenutzerkonten über Kontendefinitionen zu erstellen

1. Erstellen Sie eine Kontendefinition und weisen Sie die Automatisierungsgrade **Unmanaged** und **Full managed** zu.
2. Legen Sie für jeden Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die

Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll.

3. Erstellen Sie eine Abbildungsvorschrift für die IT Betriebsdaten.

   Mit der Abbildungsvorschrift legen Sie fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über primären Rollen einer Person ermittelt werden können.

   Welche IT Betriebsdaten erforderlich sind, ist abhängig vom Zielsystem. Für Standardbenutzerkonten werden folgende Einstellungen empfohlen:

   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IsGroupAccount` den Standardwert **1** und aktivieren Sie die Option **Immer Standardwert verwenden**.
   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IdentityType` den Standardwert **Primary** und aktivieren Sie die Option **Immer Standardwert verwenden**.

4. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem. Wählen Sie unter **Wirksam für** das konkrete Zielsystem.

   Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.

5. Weisen Sie die Kontendefinition an die Personen zu.

   Durch die Zuweisung der Kontendefinition an eine Person wird über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

Verwandte Themen

- Kontendefinitionen für PAM Benutzerkonten auf Seite 57

Administrative Benutzerkonten

Für bestimmte administrative Aufgaben, ist der Einsatz administrativer Benutzerkonten notwendig. Administrative Benutzerkonten werden in der Regel vom Zielsystem vorgegeben und haben feste Bezeichnungen und Anmeldenamen, wie beispielsweise **Administrator**.

Administrative Benutzerkonten werden durch die Synchronisation in den One Identity Manager eingelesen.

HINWEIS: Einige administrative Benutzerkonten können automatisch als privilegierte Benutzerkonten gekennzeichnet werden. Aktivieren Sie dazu im Designer den Zeitplan **Ausgewählte Benutzerkonten als privilegiert kennzeichnen**.

Verwandte Themen

- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 89
- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 90

Administrative Benutzerkonten für eine Person bereitstellen

Voraussetzungen

- Das Benutzerkonto muss als persönliche Administratoridentität gekennzeichnet sein.
- Die Person, die das Benutzerkonto nutzen soll, muss als persönliche Administratoridentität gekennzeichnet sein.
- Die Person, die das Benutzerkonto nutzen soll, muss mit einer Hauptidentität verbunden sein.

Um ein administratives Benutzerkonto für eine Person bereitzustellen

1. Kennzeichnen Sie das Benutzerkonto als persönliche Administratoridentität.
    a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Identität** den Wert **Persönliche Administratoridentität**.
2. Verbinden Sie das Benutzerkonto mit der Person, die dieses administrative Benutzerkonto nutzen soll.
    a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Person** die Person, die dieses administrative Benutzerkonto nutzt.

    > TIPP: Als Zielsystemverantwortlicher können Sie über die Schaltfläche eine neue Person erstellen.

Verwandte Themen

- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 90
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Administrative Benutzerkonten für mehrere Personen bereitstellen

Voraussetzung

- Das Benutzerkonto muss als Gruppenidentität gekennzeichnet sein.
- Es muss eine Pseudo-Person vorhanden sein. Die Pseudo-Person muss als Gruppenidentität gekennzeichnet sein und muss einen Manager besitzen.
- Die Personen, die das Benutzerkonto nutzen dürfen, müssen als primäre Identitäten gekennzeichnet sein.

Um ein administratives Benutzerkonto für mehrere Personen bereitzustellen

1. Kennzeichnen Sie das Benutzerkonto als Gruppenidentität.
    a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Identität** den Wert **Gruppenidentität**.
2. Verbinden Sie das Benutzerkonto mit einer Pseudo-Person.
    a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Person** die Pseudo-Person.

    TIPP: Als Zielsystemverantwortlicher können Sie über die Schaltfläche eine neue Pseudo-Person erstellen.
3. Weisen Sie dem Benutzerkonto die Personen zu, die dieses administrative Benutzerkonto nutzen sollen.
    a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Personen mit Nutzungsberechtigungen zuzuweisen**.
    d. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Person und doppelklicken Sie .

Verwandte Themen

- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 89
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Privilegierte Benutzerkonten

Privilegierte Benutzerkonten werden eingesetzt, um Personen mit zusätzlichen privilegierten Berechtigungen auszustatten. Dazu gehören beispielsweise administrative Benutzerkonten oder Dienstkonten. Die Benutzerkonten werden mit der Eigenschaft **Privilegiertes Benutzerkonto** (Spalte `IsPrivilegedAccount`) gekennzeichnet.

HINWEIS: Die Kriterien anhand derer Benutzerkonten automatisch als privilegiert erkannt werden, sind als Erweiterungen zur Sichtdefinition (ViewAddOn) an der Tabelle `TSBVAccountIsPrivDetectRule` (Tabelle vom Typ **Union**) definiert. Die Auswertung erfolgt im Skript `TSB_SetIsPrivilegedAccount`.

Um privilegierte Benutzerkonten über Kontendefinitionen zu erstellen

1. Erstellen Sie eine Kontendefinition. Erstellen Sie einen neuen Automatisierungsgrad für privilegierte Benutzerkonten und weisen Sie diesen Automatisierungsgrad an die Kontendefinition zu.
2. Wenn Sie verhindern möchten, dass die Eigenschaften für privilegierte Benutzerkonten überschrieben werden, setzen Sie für den Automatisierungsgrad die Eigenschaft **IT Betriebsdaten überschreibend** auf den Wert **Nur initial**. In diesem Fall werden die Eigenschaften einmalig beim Erstellen der Benutzerkonten befüllt.
3. Legen Sie für den Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll.
4. Erstellen Sie eine Abbildungsvorschrift für die IT Betriebsdaten.

   Mit der Abbildungsvorschrift legen Sie fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden, und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über primären Rollen einer Person ermittelt werden können.

   Welche IT Betriebsdaten erforderlich sind, ist abhängig vom Zielsystem. Für privilegierte Benutzerkonten werden folgende Einstellungen empfohlen:

   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IsPrivilegedAccount` den Standardwert **1** und aktivieren Sie die Option **Immer Standardwert**

verwenden.

- Zusätzlich können Sie eine Abbildungsvorschrift für die Spalte `IdentityType` festlegen. Die Spalte besitzt verschiedene zulässige Werte, die privilegierte Benutzerkonten repräsentieren.
- Um zu verhindern, das privilegierte Benutzerkonten die Berechtigungen des Standardbenutzers erben, definieren Sie eine Abbildungsvorschrift für die Spalte `IsGroupAccount` mit dem Standardwert **0** und aktivieren Sie die Option **Immer Standardwert verwenden**.

5. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem.

   Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.

6. Weisen Sie die Kontendefinition direkt an die Personen zu, die mit privilegierten Benutzerkonten arbeiten sollen.

   Durch die Zuweisung der Kontendefinition an eine Person wird über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

TIPP: Wenn es unternehmensspezifisch erforderlich ist, dass die Anmeldenamen privilegierter Benutzerkonten einem definierten Namensschema folgen, legen Sie die Bildungsregel fest, nach der die Anmeldenamen gebildet werden.

Verwandte Themen

- Kontendefinitionen für PAM Benutzerkonten auf Seite 57

Löschverzögerung für PAM Benutzerkonten festlegen

Über die Löschverzögerung legen Sie fest, wie lange die Benutzerkonten nach dem Auslösen des Löschens in der Datenbank verbleiben, bevor sie endgültig entfernt werden. Standardmäßig werden Benutzerkonten mit einer Löschverzögerung von 30 Tagen endgültig aus der Datenbank entfernt. Die Benutzerkonten werden zunächst deaktiviert oder gesperrt. Bis zum Ablauf der Löschverzögerung besteht die Möglichkeit die Benutzerkonten wieder zu aktivieren. Nach Ablauf der Löschverzögerung werden die Benutzerkonten aus der Datenbank gelöscht und ein Wiederherstellen ist nicht mehr möglich.

Sie haben die folgenden Möglichkeiten die Löschverzögerung zu konfigurieren.

- Globale Löschverzögerung: Die Löschverzögerung gilt für die Benutzerkonten in allen Zielsystemen. Der Standardwert ist **30** Tage.

Erfassen Sie eine abweichende Löschverzögerung im Designer für die Tabelle PAGUser in der Eigenschaft **Löschverzögerungen [Tage]**.

- Objektspezifische Löschverzögerung: Die Löschverzögerung kann abhängig von bestimmten Eigenschaften der Benutzerkonten konfiguriert werden.

  Um eine objektspezifische Löschverzögerung zu nutzen, erstellen Sie im Designer für die Tabelle PAGUser ein **Skript (Löschverzögerung)**.

  Beispiel:

  Die Löschverzögerung für privilegierte Benutzerkonten soll 10 Tage betragen. An der Tabelle wird folgendes **Skript (Löschverzögerung)** eingetragen.

  ```
  If $IsPrivilegedAccount:Bool$ Then
       Value = 10
  End If
  ```

Ausführliche Informationen zum Bearbeiten der Tabellendefinitionen und zum Konfigurieren der Löschverzögerung im Designer finden Sie im *One Identity Manager Konfigurationshandbuch*.

Managen von Zuweisungen von PAM Benutzergruppen

Um beispielsweise ein Kennwort für einen Assetkonto oder eine Sitzung für die Konten und Assets im Privileged Account Management System anfordern zu können, benötigen die Benutzer die erforderlichen Nutzungsrechte. Zur vereinfachten Administration können Benutzerkonten in Benutzergruppen zusammengefasst werden. Über die Benutzergruppen erhalten Benutzerkonten die Nutzungsrechte, um die Kennwörter oder Sitzungen anfordern.

Im One Identity Manager können Sie die Benutzergruppen direkt an die Benutzerkonten zuweisen oder über Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen vererben. Des Weiteren können Benutzer die Benutzergruppen über das Web Portal bestellen. Dazu werden die Benutzergruppen im IT Shop bereitgestellt.

Die Zuweisung der Nutzungsrechte an die Benutzergruppen erfolgt nicht im One Identity Manager, sondern im Privileged Account Management System.

Detaillierte Informationen zum Thema

- Zuweisen von PAM Benutzergruppen an PAM Benutzerkonten im One Identity Manager auf Seite 94
- Wirksamkeit von Mitgliedschaften in PAM Benutzergruppen auf Seite 105
- Vererbung von PAM Benutzergruppen anhand von Kategorien auf Seite 108
- Übersicht aller Zuweisungen auf Seite 110

Zuweisen von PAM Benutzergruppen an PAM Benutzerkonten im One Identity Manager

Im One Identity Manager können PAM Benutzergruppen direkt oder indirekt an Benutzerkonten zugewiesen werden.

Bei der indirekten Zuweisung werden Personen und PAM Benutzergruppen in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der PAM Benutzergruppen, die einer Person zugewiesen ist. Wenn die Person ein PAM Benutzerkonto besitzt, dann erhält dieses PAM Benutzerkonto die PAM Benutzergruppen.

Des Weiteren können Benutzergruppen im Web Portal bestellt werden. Dazu werden Personen als Kunden in einen Shop aufgenommen. Alle PAM Benutzergruppen , die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte PAM Benutzergruppen werden nach erfolgreicher Genehmigung den Personen zugewiesen.

Über Systemrollen können PAM Benutzergruppen zusammengefasst und als Paket an Personen zugewiesen werden. Sie können Systemrollen erstellen, die ausschließlich PAM Benutzergruppen enthalten. Ebenso können Sie in einer Systemrolle beliebige Unternehmensressourcen zusammenfassen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die PAM Benutzergruppen auch direkt an PAM Benutzerkonten zuweisen.

Ausführliche Informationen finden Sie in den folgenden Handbüchern.

Thema	Handbuch
Grundlagen zur Zuweisung von Unternehmensressourcen und zur Vererbung von Unternehmensressourcen	*One Identity Manager Administrationshandbuch für das Identity Management Basismodul* *One Identity Manager Administrationshandbuch für Geschäftsrollen*
Zuweisung von Unternehmensressourcen über IT Shop-Bestellungen	*One Identity Manager Administrationshandbuch für IT Shop*
Systemrollen	*One Identity Manager Administrationshandbuch für Systemrollen*

Detaillierte Informationen zum Thema

- Voraussetzungen für indirekte Zuweisungen von PAM Gruppen an PAM Benutzerkonten auf Seite 96
- PAM Benutzergruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 97
- PAM Benutzergruppen an Geschäftsrollen zuweisen auf Seite 98
- PAM Benutzergruppen in Systemrollen aufnehmen auf Seite 99
- PAM Benutzergruppen in den IT Shop aufnehmen auf Seite 100
- Lokale PAM Benutzergruppen automatisch in den IT Shop aufnehmen auf Seite 102
- PAM Benutzerkonten direkt an eine PAM Benutzergruppe zuweisen auf Seite 104
- PAM Benutzergruppen direkt an ein PAM Benutzerkonto zuweisen auf Seite 104

Voraussetzungen für indirekte Zuweisungen von PAM Gruppen an PAM Benutzerkonten

Bei der indirekten Zuweisung werden Personen und PAM Gruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen eingeordnet. Für die indirekte Zuweisung von PAM Gruppen prüfen Sie folgende Einstellungen und passen Sie die Einstellungen bei Bedarf an.

1. Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und PAM Benutzergruppen erlaubt.

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

   Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

   1. Wählen Sie im Manager in der Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.

      - ODER -

      Wählen Sie im Manager in der Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.
   2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
      - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
      - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
   3. Speichern Sie die Änderungen.
2. Einstellungen für die Zuweisung von PAM Benutzergruppen an PAM Benutzerkonten.
   - Das PAM Benutzerkonto ist mit der Option **Gruppen erbbar** gekennzeichnet.
   - Das PAM Benutzerkonto ist mit einer Person verbunden.
   - Das PAM Benutzerkonto und die PAM Benutzergruppe gehören zur selben Appliance.

HINWEIS: Bei der Vererbung von Unternehmensressourcen über Abteilungen, Kostenstellen, Standorte und Geschäftsrollen spielen unter Umständen weitere Konfigurationseinstellungen eine Rolle. So kann beispielsweise die Vererbung für eine Rolle blockiert sein oder die Vererbung an Personen nicht erlaubt sein. Ausführliche Informationen über die Grundlagen zur Zuweisung von Unternehmensressourcen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- Stammdaten für PAM Benutzerkonten bearbeiten auf Seite 137
- Allgemeine Stammdaten für PAM Benutzerkonten auf Seite 138
- Stammdaten für PAM Benutzergruppen bearbeiten auf Seite 150
- Allgemeine Stammdaten für PAM Benutzergruppen auf Seite 150

PAM Benutzergruppen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die PAM Benutzergruppen an Abteilungen, Kostenstellen oder Standorte zu, damit die PAM Benutzergruppe über diese Organisationen an PAM Benutzerkonten wird.

Um eine Gruppe an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzergruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
    - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
    - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
    - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

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

    Um eine Zuweisung zu entfernen

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

Um Gruppen an eine Abteilung, eine Kostenstelle oder einen Standort zuzuweisen (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Organisationen > Abteilungen**.

    - ODER -

    Wählen Sie im Manager die Kategorie **Organisationen > Kostenstellen**.

    - ODER -

    Wählen Sie im Manager die Kategorie **Organisationen > Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.

3. Wählen Sie die Aufgabe **PAM Benutzergruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von PAM Gruppen an PAM Benutzerkonten auf Seite 96
- PAM Benutzergruppen an Geschäftsrollen zuweisen auf Seite 98PAM Benutzergruppen an Geschäftsrollen zuweisen auf Seite 98
- PAM Benutzergruppen in Systemrollen aufnehmen auf Seite 99
- PAM Benutzergruppen in den IT Shop aufnehmen auf Seite 100
- PAM Benutzerkonten direkt an eine PAM Benutzergruppe zuweisen auf Seite 104
- PAM Benutzergruppen direkt an ein PAM Benutzerkonto zuweisen auf Seite 104
- One Identity Manager Benutzer für die Verwaltung eines Privileged Account Management Systems auf Seite 11

PAM Benutzergruppen an Geschäftsrollen zuweisen

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

Weisen Sie die PAM Benutzergruppe an Geschäftsrollen zu, damit die PAM Benutzergruppe über diese Geschäftsrollen an PAM Benutzerkonten zugewiesen wird.

Um eine Gruppe an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzergruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Um Gruppen an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen > <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe**PAM Benutzergruppen zuweisen**.

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

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie ✓.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von PAM Gruppen an PAM Benutzerkonten auf Seite 96
- PAM Benutzergruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 97
- PAM Benutzergruppen in Systemrollen aufnehmen auf Seite 99
- PAM Benutzergruppen in den IT Shop aufnehmen auf Seite 100
- PAM Benutzerkonten direkt an eine PAM Benutzergruppe zuweisen auf Seite 104
- PAM Benutzergruppen direkt an ein PAM Benutzerkonto zuweisen auf Seite 104
- One Identity Manager Benutzer für die Verwaltung eines Privileged Account Management Systems auf Seite 11

PAM Benutzergruppen in Systemrollen aufnehmen

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

Mit dieser Aufgabe nehmen Sie eine Gruppe in Systemrollen auf.

Wenn Sie eine Systemrolle an Personen zuweisen, wird die Gruppe an alle PAM Benutzerkonten vererbt, die diese Personen besitzen.

HINWEIS: Gruppen, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können nur an Systemrollen zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Systemrollen*.

Um eine Gruppe an Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzergruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemrolle und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von PAM Gruppen an PAM Benutzerkonten auf Seite 96
- PAM Benutzergruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 97
- PAM Benutzergruppen an Geschäftsrollen zuweisen auf Seite 98
- PAM Benutzergruppen in den IT Shop aufnehmen auf Seite 100
- PAM Benutzerkonten direkt an eine PAM Benutzergruppe zuweisen auf Seite 104
- PAM Benutzergruppen direkt an ein PAM Benutzerkonto zuweisen auf Seite 104

PAM Benutzergruppen in den IT Shop aufnehmen

Mit der Zuweisung einer Benutzergruppe an ein IT Shop Regal kann sie von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Die Benutzergruppe muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Benutzergruppe muss eine Leistungsposition zugeordnet sein.

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Benutzergruppe im Web Portal leichter gefunden

werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.

- Soll die Benutzergruppe nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss die Benutzergruppe zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen oder Benutzerkonten ist dann nicht mehr zulässig.

HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren Benutzergruppen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Benutzergruppen in den IT Shop aufzunehmen.

Um eine Gruppe eine Benutzergruppe in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzergruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > PAM Benutzergruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Benutzergruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Wählen Sie den Tabreiter **IT Shop Strukturen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzergruppe an die IT Shop Regale zu.
6. Speichern Sie die Änderungen.

Um eine Benutzergruppe aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzergruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > PAM Benutzergruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Benutzergruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Wählen Sie den Tabreiter **IT Shop Strukturen**.
5. Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzergruppe aus den IT Shop Regalen.
6. Speichern Sie die Änderungen.

Um eine Benutzergruppe aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzergruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

Wählen Sie im Manager die Kategorie **Berechtigungen > PAM Benutzergruppen** (bei rollenbasierter Anmeldung).

2. Wählen Sie in der Ergebnisliste die Benutzergruppe.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Die Benutzergruppe wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Benutzergruppe abbestellt.

Ausführliche Informationen zur Bestellung von Unternehmensressourcen über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von PAM Gruppen an PAM Benutzerkonten auf Seite 96
- Lokale PAM Benutzergruppen automatisch in den IT Shop aufnehmen auf Seite 102
- Allgemeine Stammdaten für PAM Benutzergruppen auf Seite 150
- PAM Benutzergruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 97
- PAM Benutzergruppen an Geschäftsrollen zuweisen auf Seite 98
- PAM Benutzergruppen in Systemrollen aufnehmen auf Seite 99
- PAM Benutzerkonten direkt an eine PAM Benutzergruppe zuweisen auf Seite 104
- PAM Benutzergruppen direkt an ein PAM Benutzerkonto zuweisen auf Seite 104
- One Identity Manager Benutzer für die Verwaltung eines Privileged Account Management Systems auf Seite 11

Lokale PAM Benutzergruppen automatisch in den IT Shop aufnehmen

Mit den folgenden Schritten können Sie lokale PAM Benutzergruppen automatisch in den IT Shop aufnehmen. Die Synchronisation sorgt dafür, dass die Benutzergruppen in den IT Shop aufgenommen werden. Bei Bedarf können Sie die Synchronisation im Synchronization Editor sofort starten.

HINWEIS: Verzeichnisgruppen werden nicht automatisch in den IT Shop aufgenommen.

Um lokale PAM Benutzergruppen automatisch in den IT Shop aufzunehmen

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER| ITShop | AutoPublish | PAGUsrGroup**.

   Die lokalen PAM Benutzergruppen werden ab diesem Zeitpunkt automatisch in den IT Shop aufgenommen.

2. Um einzelne lokale PAM Benutzergruppen nicht automatisch in den IT Shop aufzunehmen, aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | PAGUsrGroup | ExcludeList**.

   Der Konfigurationsparameter enthält eine Auflistung aller PAM Benutzergruppen, die nicht automatisch zum IT Shop zugeordnet werden sollen.

   Bei Bedarf können Sie die Liste erweitern. Erfassen Sie dazu im Wert des Konfigurationsparameters die Namen der Benutzergruppen. Die Angabe der Namen erfolgt in einer Pipe (|) getrennten Liste.

3. Weisen Sie die Personen, die über die Bestellung der lokalen Benutzergruppen entscheiden dürfen, der Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner | PAM Benutzergruppen** zu. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop.*

   Über die Entscheidungsrichtlinie **Entscheidung der Bestellungen von PAM Benutzergruppenmitgliedschaften** werden die Produkteigner der Benutzergruppen als Entscheider ermittelt. Können keine Produkteigner ermittelt werden, werden die Bestellungen den Zielsystemverantwortlichen zur Entscheidung vorgelegt.

Folgende Schritte werden bei der Aufnahme einer lokalen PAM Benutzergruppe in den IT Shop automatisch ausgeführt.

1. Es wird eine Leistungsposition für die Benutzergruppe ermittelt.

   Für jede Benutzergruppe wird die Leistungsposition geprüft und bei Bedarf angepasst. Die Bezeichnung der Leistungsposition entspricht der Gruppenbezeichnung.

   - Für Gruppen mit Leistungsposition wird die Leistungsposition angepasst.
   - Gruppen ohne Leitungsposition erhalten eine neue Leistungsposition.

2. Die Leistungsposition wird der Standard-Servicekategorie **PAM Benutzergruppen** zugeordnet.
3. Die Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner | PAM Benutzergruppen** wird als Produkteigner an die Leistungsposition zugeordnet.
4. Die Benutzergruppe wird mit der Option **IT Shop** gekennzeichnet und dem IT Shop Regal **PAM Benutzergruppen** im Shop **Identity & Access Lifecycle** zugewiesen.

Anschließend können die Kunden des Shops Gruppenmitgliedschaften über das Web Portal bestellen.

Ausführliche Informationen zur Konfiguration des IT Shops finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*. Ausführliche Informationen zum Bestellen von Zugriffsanforderungen im Web Portal finden Sie im *One Identity Manager Web Portal Anwenderhandbuch*.

Verwandte Themen

- PAM Benutzergruppen in den IT Shop aufnehmen auf Seite 100
- Allgemeine Stammdaten für PAM Benutzergruppen auf Seite 150

PAM Benutzerkonten direkt an eine PAM Benutzergruppe zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Gruppen direkt an Benutzerkonten zuweisen. Gruppen, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Um Benutzerkonten direkt an eine Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzergruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- PAM Benutzergruppen direkt an ein PAM Benutzerkonto zuweisen auf Seite 104
- PAM Benutzergruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 97
- PAM Benutzergruppen an Geschäftsrollen zuweisen auf Seite 98
- PAM Benutzergruppen in Systemrollen aufnehmen auf Seite 99
- PAM Benutzergruppen in den IT Shop aufnehmen auf Seite 100

PAM Benutzergruppen direkt an ein PAM Benutzerkonto zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Gruppen direkt an Benutzerkonten zuweisen. Gruppen, die mit der Option **Verwendung nur im IT Shop**

gekennzeichnet sind, können nicht direkt zugewiesen werden.

Um Gruppen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- PAM Benutzerkonten direkt an eine PAM Benutzergruppe zuweisen auf Seite 104
- PAM Benutzergruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 97
- PAM Benutzergruppen an Geschäftsrollen zuweisen auf Seite 98
- PAM Benutzergruppen in Systemrollen aufnehmen auf Seite 99
- PAM Benutzergruppen in den IT Shop aufnehmen auf Seite 100

Wirksamkeit von Mitgliedschaften in PAM Benutzergruppen

Bei der Zuweisung von Gruppen an Benutzerkonten kann es vorkommen, dass eine Person zwei oder mehr Gruppen erhält, die in dieser Kombination nicht auftreten dürfen. Um das zu verhindern, geben Sie die sich ausschließenden Gruppen bekannt. Dabei legen Sie für zwei Gruppen fest, welche der beiden Gruppen an Benutzerkonten wirksam werden soll, wenn beide zugewiesen sind.

Die Zuweisung einer ausgeschlossenen Gruppe ist jederzeit direkt, indirekt oder per IT Shop-Bestellung möglich. Anschließend ermittelt der One Identity Manager, ob diese Zuweisung wirksam ist.

HINWEIS:

- Ein wechselseitiger Ausschluss zweier Gruppen kann nicht definiert werden. Das heißt, die Festlegung "Gruppe A schließt Gruppe B aus" UND "Gruppe B schließt Gruppe A aus" ist nicht zulässig.

- Für eine Gruppe muss jede auszuschließende Gruppe einzeln bekannt gegeben werden. Ausschlussdefinitionen werden nicht vererbt.

Die Wirksamkeit der Zuweisungen wird in den Tabellen `PAGUserInUsrGroup` und `PAGBaseTreeHasUsrGroup` über die Spalte `XIsInEffect` abgebildet.

Beispiel: Wirksamkeit von Gruppenmitgliedschaften

- In einer Appliance ist eine Gruppe A mit Berechtigungen zum Auslösen von Bestellungen definiert. Eine Gruppe B berechtigt zum Anweisen von Zahlungen. Eine Gruppe C berechtigt zum Prüfen von Rechnungen.
- Gruppe A wird über die Abteilung "Marketing", Gruppe B über die Abteilung "Finanzen" und Gruppe C wird über die Geschäftsrolle "Kontrollgruppe" zugewiesen.

Clara Harris hat ein Benutzerkonto in dieser Appliance. Sie gehört primär der Abteilung "Marketing" an. Sekundär sind ihr die Geschäftsrolle "Kontrollgruppe" und die Abteilung "Finanzen" zugewiesen. Ohne Ausschlussdefinition erhält das Benutzerkonto alle Berechtigungen der Gruppen A, B und C.

Durch geeignete Maßnahmen soll verhindert werden, dass eine Person gleichzeitig die Berechtigungen der Gruppe A und der Gruppe B erhält. Das heißt, die Gruppen A und B schließen sich aus. Ein Benutzer, der Mitglied der Gruppe C ist, darf ebenfalls nicht gleichzeitig Mitglied der Gruppe B sein. Das heißt, die Gruppen B und C schließen sich aus.

Tabelle 12: Festlegen der ausgeschlossenen Gruppen (Tabelle `PAGUsrGroupExclusion`)

Wirksame Gruppe	Ausgeschlossene Gruppe
Gruppe A	
Gruppe B	Gruppe A
Gruppe C	Gruppe B

Tabelle 13: Wirksame Zuweisungen

Person	Mitglied in Rolle	Wirksame Gruppe
Ben King	Marketing	Gruppe A
Jan Bloggs	Marketing, Finanzen	Gruppe B
Clara Harris	Marketing, Finanzen, Kontrollgruppe	Gruppe C
Jenny Basset	Marketing, Kontrollgruppe	Gruppe A, Gruppe C

Für Clara Harris ist nur die Zuweisung der Gruppe C wirksam und wird ins Zielsystem publiziert. Verlässt Clara Harris die Geschäftsrolle "Kontrollgruppe" zu einem späteren Zeitpunkt, wird die Gruppe B ebenfalls wirksam.

Für Jenny Basset sind die Gruppen A und C wirksam, da zwischen beiden Gruppen kein Ausschluss definiert wurde. Soll das verhindert werden, definieren Sie einen weiteren Ausschluss für die Gruppe C.

Tabelle 14: Ausgeschlossene Gruppen und wirksame Zuweisungen

Person	Mitglied in Rolle	Zugewiesene Gruppe	Ausgeschlossene Gruppe	Wirksame Gruppe
Jenny Basset	Marketing	Gruppe A		Gruppe C
	Kontrollgruppe	Gruppe C	Gruppe B	
			Gruppe A	

Voraussetzungen

- Der Konfigurationsparameter **QER | Structures | Inherite | GroupExclusion** ist aktiviert.

  Aktivieren Sie im Designer den Konfigurationsparameter und kompilieren Sie die Datenbank.

  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*.
- Sich ausschließende Gruppen gehören zur selben Appliance.

Um Gruppen auszuschließen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzergruppen**.
2. Wählen Sie in der Ergebnisliste eine Gruppe.
3. Wählen Sie die Aufgabe **Gruppen ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu, die sich mit der gewählten Gruppe ausschließen.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

Vererbung von PAM Benutzergruppen anhand von Kategorien

Im One Identity Manager können Benutzergruppen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Benutzergruppen und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält zwei Tabellen; die Benutzerkontentabelle und die Gruppentabelle. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In der Gruppentabelle geben Sie Ihre Kategorien für die zielsystemabhängigen Gruppen an. In den übrigen Tabellen geben Sie Ihre Kategorien für die Benutzergruppen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 63**.

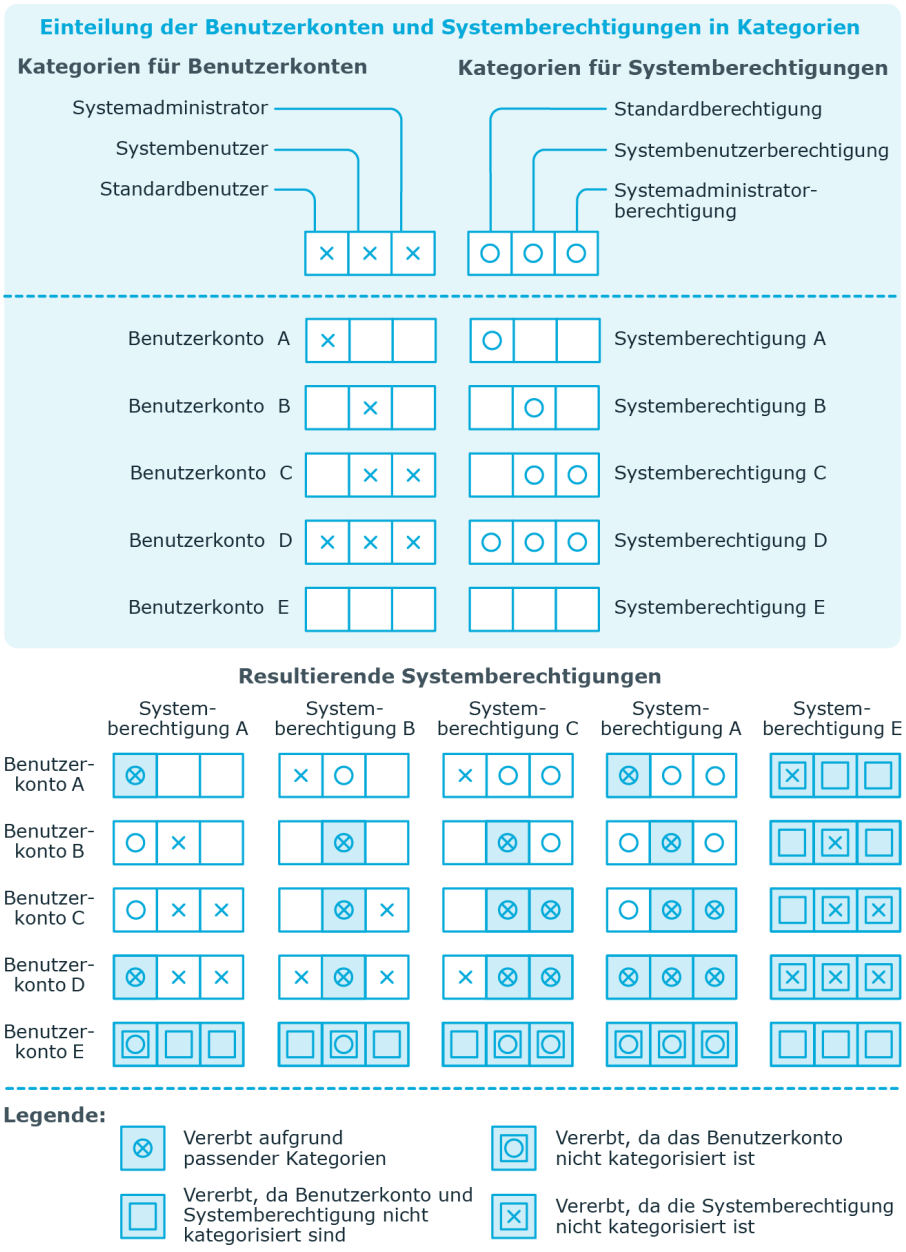
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Berechtigung kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Berechtigung überein, wird die Berechtigung an das Benutzerkonto vererbt. Ist die Berechtigung oder das Benutzerkonto nicht in Kategorien eingestuft, dann wird die Berechtigung ebenfalls an das Benutzerkonto vererbt.

HINWEIS: Die Vererbung über Kategorien wird nur bei der indirekten Zuweisung von Berechtigungen über hierarchische Rollen berücksichtigt. Bei der direkten Zuweisung von Berechtigungen an Benutzerkonten werden die Kategorien nicht berücksichtigt.

Tabelle 15: Beispiele für Kategorien

Kategorieposition	Kategorien für Benutzerkonten	Kategorien für Berechtigungen
1	Standardbenutzer	Standardgruppe oder Standardprodukt
2	Administrator	Administratorgruppe

Abbildung 1: Beispiel für die Vererbung über Kategorien



Um die Vererbung über Kategorien zu nutzen

1. Definieren Sie an der Appliance die Kategorien.
2. Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
3. Weisen Sie die Kategorien den Gruppen über ihre Stammdaten zu.

Verwandte Themen

- Kategorien für die Vererbung von PAM Benutzergruppen definieren auf Seite 131
- Allgemeine Stammdaten für PAM Benutzerkonten auf Seite 138
- Allgemeine Stammdaten für PAM Benutzergruppen auf Seite 150

Übersicht aller Zuweisungen

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

Beispiele:

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

Um detaillierte Informationen über Zuweisungen anzuzeigen

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

  Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Personen befinden, denen das ausgewählte Basisobjekt zugewiesen ist. Die Bedeutung der Steuerelemente des Berichts ist in einer separaten Legende erläutert. Die Legende erreichen Sie über das Symbol in der Symbolleiste des Berichtes.

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

Abbildung 2: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 16: Bedeutung der Symbole in der Symbolleiste des Berichts

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

6

Bereitstellen von Anmeldeinformationen für PAM Benutzerkonten

Wenn neue Benutzerkonten im One Identity Manager angelegt werden, werden sofort auch die zur Anmeldung am Zielsystem benötigten Kennwörter erstellt. Um das initiale Kennwort zu vergeben, stehen verschiedene Möglichkeiten zur Verfügung. Auf die Kennwörter werden vordefinierte Kennwortrichtlinien angewendet, die Sie bei Bedarf an Ihre Anforderungen anpassen können. Um die generierten Anmeldeinformationen an die Benutzer zu verteilen, können Sie E-Mail-Benachrichtigungen einrichten.

Detaillierte Informationen zum Thema

- Kennwortrichtlinien für PAM Benutzer auf Seite 112
- Initiales Kennwort für neue PAM Benutzerkonten auf Seite 124
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 125

Kennwortrichtlinien für PAM Benutzer

Der One Identity Manager unterstützt Sie beim Erstellen von komplexen Kennwortrichtlinien beispielsweise für Systembenutzerkennwörter, das zentrale Kennwort von Personen sowie für Kennwörter für die einzelnen Zielsysteme. Kennwortrichtlinien werden sowohl bei der Eingabe eines Kennwortes durch den Anwender als auch bei der Generierung von Zufallskennwörtern angewendet.

In der Standardinstallation werden vordefinierte Kennwortrichtlinien mitgeliefert, die Sie nutzen können und bei Bedarf an Ihre Anforderungen anpassen können. Zusätzlich können Sie eigene Kennwortrichtlinien definieren.

Detaillierte Informationen zum Thema

- Vordefinierte Kennwortrichtlinien auf Seite 113
- Kennwortrichtlinien anwenden auf Seite 114

- Kennwortrichtlinien bearbeiten auf Seite 116
- Kennwortrichtlinien erstellen auf Seite 116
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 120
- Ausschlussliste für Kennwörter bearbeiten auf Seite 123
- Kennwörter prüfen auf Seite 123
- Generieren von Kennwörtern testen auf Seite 124

Vordefinierte Kennwortrichtlinien

Die vordefinierten Kennwortrichtlinien können Sie bei Bedarf an Ihre Anforderungen anpassen.

Kennwortrichtlinie für die Anmeldung am One Identity Manager

Für die Anmeldung am One Identity Manager wird die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** angewendet. Diese Kennwortrichtlinie definiert die Einstellung für die Kennwörter von Systembenutzern (`DialogUser.Password` und `Person.DialogUserPassword`) sowie für den Zugangscode für die einmalige Anmeldung am Web Portal (`Person.Passcode`).

HINWEIS: Die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn keine andere Kennwortrichtlinie für Personen, Benutzerkonten oder Systembenutzer ermittelt werden kann.

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

Kennwortrichtlinie für die Bildung des zentralen Kennwortes von Personen

Bei entsprechender Konfiguration wird das zentrale Kennwort einer Person auf die Kennwörter der zielsystemspezifischen Benutzerkonten abgebildet. Die Kennwortrichtlinie **Kennwortrichtlinie für zentrales Kennwort von Personen** definiert die Einstellung für das zentrale Kennwort (`Person.CentralPassword`). Die Mitglieder der Anwendungsrolle **Identity Management | Personen | Administratoren** können diese Kennwortrichtlinie anpassen.

WICHTIG: Stellen Sie sicher, dass die Kennwortrichtlinie **Kennwortrichtlinie für zentrales Kennwort von Personen** nicht gegen die zielsystemspezifischen Anforderungen an Kennwörter verstößt.

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

Kennwortrichtlinien für Benutzerkonten

Es werden vordefinierte Kennwortrichtlinien bereitgestellt, die Sie auf die Kennwortspalten der Benutzerkonten anwenden können.

WICHTIG: Wenn Sie nicht mit zielsystemspezifischen Kennwortrichtlinien arbeiten, wirkt die Standardrichtlinie **One Identity Manager Kennwortrichtlinie**. Stellen Sie in diesem Fall sicher, dass die Standardrichtlinie nicht gegen die Anforderungen der Zielsysteme verstößt.

Für Privileged Account Management Systeme ist die Kennwortrichtlinie **PAM Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Benutzerkonten (`PAGUser.Password`) einer Appliance anwenden.

Wenn die Kennwortanforderungen der Appliances unterschiedlich sind, wird empfohlen, je Appliance eine eigene Kennwortrichtlinie einzurichten.

Des Weiteren können Sie Kennwortrichtlinien abhängig von der Kontendefinition der Benutzerkonten oder abhängig vom Automatisierungsgrad der Benutzerkonten anwenden.

Kennwortrichtlinien anwenden

Für Privileged Account Management Systeme ist die Kennwortrichtlinie **PAM Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Benutzerkonten (`PAGUser.Password`) einer Appliance anwenden.

Wenn die Kennwortanforderungen der Appliances unterschiedlich sind, wird empfohlen, je Appliance eine eigene Kennwortrichtlinie einzurichten.

Des Weiteren können Sie Kennwortrichtlinien abhängig von der Kontendefinition der Benutzerkonten oder abhängig vom Automatisierungsgrad der Benutzerkonten anwenden.

Die anzuwendende Kennwortrichtlinie für ein Benutzerkonto wird in folgender Reihenfolge ermittelt:

1. Kennwortrichtlinie der Kontendefinition des Benutzerkontos.
2. Kennwortrichtlinie des Automatisierungsgrades des Benutzerkontos.
3. Kennwortrichtlinie der Appliance des Benutzers.
4. Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** (Standardrichtlinie).

WICHTIG: Wenn Sie nicht mit zielsystemspezifischen Kennwortrichtlinien arbeiten, wirkt die Standardrichtlinie **One Identity Manager Kennwortrichtlinie**. Stellen Sie in diesem Fall sicher, dass die Standardrichtlinie nicht gegen die Anforderungen der Zielsysteme verstößt.

Um eine Kennwortrichtlinie neu zuzuweisen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.

3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Klicken Sie im Bereich **Zuweisungen** die Schaltfläche **Hinzufügen** und erfassen Sie folgende Daten.
    - **Anwenden auf**: Anwendungsbereich der Kennwortrichtlinie.

      Um den Anwendungsbereich festzulegen

      1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.
      2. Wählen Sie unter **Tabelle** eine der folgenden Referenzen:
          - Die Tabelle, die die Basisobjekte der Synchronisation enthält.
          - Um die Kennwortrichtlinie abhängig von der Kontendefinition anzuwenden, wählen Sie die Tabelle **TSBAccountDef**.
          - Um die Kennwortrichtlinie abhängig vom Automatisierungsgrad anzuwenden, wählen Sie die Tabelle **TSBBehavoir**.
      3. Wählen Sie unter **Anwenden auf** die Tabelle, die die Basisobjekte enthält.
          - Wenn Sie die Tabelle mit den Basisobjekten der Synchronisation gewählt haben, dann wählen Sie das konkrete Zielsystem.
          - Wenn Sie die Tabelle **TSBAccountDef** gewählt haben, dann wählen Sie die konkrete Kontendefinition.
          - Wenn Sie die Tabelle **TSBBehavior** gewählt haben, dann wählen Sie den konkreten Automatisierungsgrad.
      4. Klicken Sie **OK**.
    - **Kennwortspalte**: Bezeichnung der Kennwortspalte.
    - **Kennwortrichtlinie**: Bezeichnung der Kennwortrichtlinie, die angewendet werden soll.
5. Speichern Sie die Änderungen.

Um die Zuweisung einer Kennwortrichtlinie zu ändern

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Wählen Sie im Bereich **Zuweisungen** die Zuweisung, die Sie ändern möchten.
5. Wählen Sie in der Auswahlliste **Kennwortrichtlinie** die neu anzuwendende Kennwortrichtlinie.
6. Speichern Sie die Änderungen.

Kennwortrichtlinien bearbeiten

In der Standardinstallation werden vordefinierte Kennwortrichtlinien mitgeliefert, die Sie nutzen können und bei Bedarf an Ihre Anforderungen anpassen können.

Um eine Kennwortrichtlinie zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten der Kennwortrichtlinie.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kennwortrichtlinien auf Seite 117
- Richtlinieneinstellungen auf Seite 117
- Zeichenklassen für Kennwörter auf Seite 119
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 120

Kennwortrichtlinien erstellen

In der Standardinstallation werden vordefinierte Kennwortrichtlinien mitgeliefert, die Sie nutzen können und bei Bedarf an Ihre Anforderungen anpassen können. Zusätzlich können Sie eigene Kennwortrichtlinien definieren.

Um eine Kennwortrichtlinie zu erstellen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular erfassen Sie die Stammdaten der Kennwortrichtlinie.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kennwortrichtlinien auf Seite 117
- Richtlinieneinstellungen auf Seite 117
- Zeichenklassen für Kennwörter auf Seite 119
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 120

Allgemeine Stammdaten für Kennwortrichtlinien

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 17: Stammdaten einer Kennwortrichtlinie

Eigenschaft	Bedeutung
Anzeigename	Bezeichnung der Kennwortrichtlinie. Übersetzen Sie den eingegebenen Text über die Schaltfläche.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.Übersetzen Sie den eingegebenen Text über die Schaltfläche.
Fehlermeldung	Kundenspezifische Fehlermeldung, die ausgegeben wird, wenn die Richtlinie nicht erfüllt wird. Übersetzen Sie den eingegebenen Text über die Schaltfläche.
Eigentümer (Anwendungsrolle)	Anwendungsrolle, deren Mitglieder die Kennwortrichtlinie konfigurieren können.
Standardrichtlinie	Kennzeichnung als Standardrichtlinie für Kennwörter. Die Option kann nicht geändert werden. HINWEIS: Die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn keine andere Kennwortrichtlinie für Personen, Benutzerkonten oder Systembenutzer ermittelt werden kann.

Richtlinieneinstellungen

Auf dem Tabreiter **Kennwort** definieren Sie folgende Einstellungen für eine Kennwortrichtlinie.

Tabelle 18: Richtlinieneinstellungen

Eigenschaft	Bedeutung
Initiales Kennwort	Initiales Kennwort für neu erzeugte Benutzerkonten. Wenn beim Erstellen eines Benutzerkontos kein Kennwort angegeben wird oder kein Zufallskennwort generiert wird, dann wird das initiale Kennwort benutzt.
Kennwortbestätigung	Kennwortwiederholung.
Min. Länge	Minimale Länge des Kennwortes. Geben Sie die Anzahl von

Eigenschaft	Bedeutung
	Zeichen an, die ein Kennwort haben muss. Ist der Wert **0**, ist kein Kennwort erforderlich.
Max. Länge	Maximale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben kann. Der maximal zulässige Wert ist **256**.
Max. Fehlanmeldungen	Anzahl der maximalen Fehlanmeldungen. Legen Sie die Anzahl der ungültigen Kennworteingaben fest. Die Anzahl der Fehlanmeldungen wird nur bei der Anmeldung am One Identity Manager berücksichtigt. Ist der Wert **0**, dann wird die Anzahl der Fehlanmeldungen nicht berücksichtigt. Die Angabe wird nur berücksichtigt, wenn die Anmeldung am One Identity Manager mit einem Systembenutzer- oder Personen-basierten Authentifizierungsmodul erfolgt. Hat ein Benutzer die Anzahl der maximalen Fehlanmeldungen überschritten, kann sich die Person oder der Systembenutzer nicht mehr am One Identity Manager anmelden. Kennwörter gesperrter Personen und Systembenutzer können im Kennwortrücksetzungsportal zurückgesetzt werden. Ausführliche Informationen finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.
Max. Tage gültig	Maximales Alter des Kennwortes. Geben Sie die Zeitspanne an, in der ein Kennwort verwendet werden kann, bevor ein neues Kennwort erwartet wird. Ist der Wert **0**, dann läuft das Kennwort nicht ab.
Kennwortchronik	Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert **5** eingegeben, werden die letzten fünf Kennwörter des Benutzers gespeichert. Ist der Wert **0**, dann werden keine Kennwörter in der Kennwortchronik gespeichert.
Min. Kennwortstärke	Gibt an, wie sicher ein Kennwort sein muss. Je höher die Kennwortstärke, desto sicherer ist das Kennwort. Mit dem Wert **0** wird die Kennwortstärke nicht geprüft. Die Werte **1**, **2**, **3** und **4** geben die erforderliche Komplexität des Kennwortes an. Dabei stellt der Wert **1** die geringsten Anforderungen an die Komplexität eines Kennwortes. Der Wert **4** fordert die höchste Komplexität.
Namensbestandteile unzulässig	Gibt an, ob Namensbestandteile im Kennwort zulässig oder unzulässig sind. Ist die Option aktiviert, sind Namensbestandteile in Kennwörtern nicht zulässig. Es werden die Werte der Spalten berücksichtigt, für welche die Option **Enthält Namensbestandteile für die**

Eigenschaft	Bedeutung
	Kennwortprüfung aktiviert ist. Die Option passen Sie im Designer an der Spaltendefinition an. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Zeichenklassen für Kennwörter

Auf dem Tabreiter **Zeichenklassen** legen Sie fest, welche Zeichen für ein Kennwort zulässig sind.

Tabelle 19: Zeichenklassen für Kennwörter

Eigenschaft	Bedeutung
Erforderliche Anzahl von Zeichenklassen	Anzahl der Regeln für Zeichenklassen, die erfüllt sein müssen, damit ein Kennwort der Kennwortrichtlinie entspricht. Berücksichtigt werden die Regeln für **Min. Anzahl Buchstaben**, **Min. Anzahl Kleinbuchstaben**, **Min. Anzahl Großbuchstaben**, **Min. Anzahl Ziffern** und **Min. Anzahl Sonderzeichen**. Es bedeuten: • Wert **0**: Es müssen alle Zeichenklassenregeln erfüllt sein. • Wert **> 0**: Anzahl der Zeichenklassenregeln, die mindestens erfüllt sein müssen. Der Wert kann maximal der Anzahl der Regeln entsprechend, deren Wert **> 0** ist. HINWEIS: Die Prüfung erfolgt nicht für generierte Kennwörter.
Min. Anzahl Buchstaben	Gibt an, wie viele alphabetische Zeichen ein Kennwort mindestens enthalten muss.
Min. Anzahl Kleinbuchstaben	Gibt an, wie viele Kleinbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Großbuchstaben	Gibt an, wie viele Großbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Ziffern	Gibt an, wie viele Ziffern ein Kennwort mindestens enthalten muss.
Min. Anzahl Sonderzeichen	Gibt an, wie viele Sonderzeichen ein Kennwort mindestens enthalten muss.
Zulässige Sonderzeichen	Liste zulässiger Sonderzeichen.
Max. identische Zeichen insgesamt	Maximale Anzahl identischer Zeichen, die insgesamt im Kennwort vorkommen dürfen.

Eigenschaft	Bedeutung
Max. identische Zeichen aufeinanderfolgend	Maximale Anzahl identischer Zeichen, die nacheinander wiederholt werden können.
Unzulässige Sonderzeichen	Liste unzulässiger Sonderzeichen.
Keine Klein-buchstaben erzeugen	Gibt an, ob ein generiertes Kennwort Kleinbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keinen Großbuch-staben erzeugen	Gibt an, ob ein generiertes Kennwort Großbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keine Ziffern erzeugen	Gibt an, ob ein generiertes Kennwort Ziffern enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berück-sichtigt.
Keine Sonderzeichen erzeugen	Gibt an, ob ein generiertes Kennwort Sonderzeichen enthalten darf. Ist die Option aktiviert, sind nur Buchstaben, Zahlen und Leerzeichen in Kennwörtern erlaubt. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.

Kundenspezifische Skripte für Kennwortanforderungen

Kundenspezifische Skripte zum Prüfen und Generieren von Kennwörtern können Sie einsetzen, wenn die Anforderungen an Kennwörter mit den vorhandenen Einstellmöglichkeiten nicht abgebildet werden können. Skripte werden zusätzlich zu den anderen Einstellungen angewendet.

Detaillierte Informationen zum Thema

- Skript zum Prüfen eines Kennwortes auf Seite 120
- Skript zum Generieren eines Kennwortes auf Seite 122

Skript zum Prüfen eines Kennwortes

Ein Prüfskript können Sie einsetzen, wenn zusätzliche Richtlinien beim Prüfen eines Kennwortes angewendet werden sollen, die nicht mit den vorhandenen Einstellmöglichkeiten abgebildet werden können.

Syntax für Prüfskripte

```
Public Sub CCC_CustomPwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd
As System.Security.SecureString)
```

Mit Parametern:

`policy` = Kennwortrichtlinienobjekt

`spwd` = Kennwort, das zu prüfen ist

TIPP: Um das Basisobjekt zu verwenden, nutzen Sie die Eigenschaft `Entity` der `PasswordPolicy`-Klasse.

Beispiel: Skript zum Prüfen eines Kennwortes

Ein Kennwort in darf nicht mit **?** oder **!** beginnen. Das Kennwort darf nicht mit drei identischen Zeichen beginnen. Das Skript prüft ein gegebenes Kennwort auf Zulässigkeit.

```
Public Sub CCC_PwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd
As System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            Throw New Exception(#LD("Password can't start with '?' or
            '!'")#)
        End If
    End If
    If pwd.Length>2
        If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
            Throw New Exception(#LD("Invalid character sequence in
            password")#)
        End If
    End If
End Sub
```

Um ein kundenspezifisches Skript zum Prüfen eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
    b. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.

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

d. Tragen Sie auf dem Tabreiter **Skripte** im Eingabefeld **Prüfskript** den Namen des Skriptes ein, das zum Prüfen eines Kennwortes verwendet wird.

e. Speichern Sie die Änderungen.

Verwandte Themen

- Skript zum Generieren eines Kennwortes auf Seite 122

Skript zum Generieren eines Kennwortes

Ein Generierungsskript können Sie einsetzen, wenn zusätzliche Richtlinien beim Generieren eines Zufallskennwortes angewendet werden sollen, die nicht mit den vorhandenen Einstellmöglichkeiten abgebildet werden können.

Syntax für Generierungsskripte

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)
```

Mit Parametern:

`policy` = Kennwortrichtlinienobjekt

`spwd` = Generiertes Kennwort

TIPP: Um das Basisobjekt zu verwenden, nutzen Sie die Eigenschaft `Entity` der `PasswordPolicy`-Klasse.

Beispiel: Skript zum Generieren eines Kennwortes

Das Skript ersetzt in Zufallskennwörtern die unzulässigen Zeichen **?** und **!** zu Beginn eines Kennwortes mit **_**.

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd
As System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    ' replace invalid characters at first position
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            spwd.SetAt(0, CChar("_"))
        End If
    End If
```

```
End Sub
```

Um ein kundenspezifisches Skript zum Generieren eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
    b. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Tragen Sie auf dem Tabreiter **Skripte** im Eingabefeld **Generierungsskript** den Namen des Skriptes ein, das zum Generieren eines Kennwortes verwendet wird.
    e. Speichern Sie die Änderungen.

Verwandte Themen

- Skript zum Prüfen eines Kennwortes auf Seite 120

Ausschlussliste für Kennwörter bearbeiten

Um bestimmte Begriffe im Kennwort zu verbieten, nehmen Sie den Begriff in die Ausschlussliste auf.

HINWEIS: Die Ausschlussliste ist global für alle Kennwortrichtlinien gültig.

Um einen Begriff in die Ausschlussliste aufzunehmen

1. Wählen Sie im Designer die Kategorie **Basisdaten > Sicherheitseinstellungen > Kennwort Ausschlussliste**.
2. Erstellen Sie einen neuen Eintrag über den Menüeintrag **Objekt > Neu** und erfassen Sie den auszuschließenden Begriff.
3. Speichern Sie die Änderungen.

Kennwörter prüfen

Beim Prüfen eines Kennwortes werden alle definierten Einstellungen der Kennwortrichtlinie, kundenspezifische Skripte sowie die Ausschlussliste für Kennwörter berücksichtigt.

Um zu prüfen, ob ein Kennwort der Kennwortrichtlinie entspricht

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Test**.
5. Wählen Sie in der Auswahlliste **Basisobjekt für den Test** die Tabelle und das Objekt für die Prüfung.
6. Geben Sie im Eingabefeld **Kennwort überprüfen** das Kennwort ein.

   Neben dem Eingabefeld wird angezeigt, ob das Kennwort gültig ist.

Generieren von Kennwörtern testen

Beim Generieren eines Kennwortes werden alle definierten Einstellungen der Kennwortrichtlinie, kundenspezifische Skripte sowie die Ausschlussliste für Kennwörter berücksichtigt.

Um ein Kennwort zu generieren, das der Kennwortrichtlinie entspricht

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Test**.
5. Klicken Sie auf die Schaltfläche **Generieren**.

   Das generierte Kennwort wird angezeigt.

Initiales Kennwort für neue PAM Benutzerkonten

Um das initiale Kennwort für neue Benutzerkonten zu vergeben, stehen Ihnen verschiedene Möglichkeiten zur Verfügung.

- Tragen Sie beim Erstellen des Benutzerkontos in den Stammdaten ein Kennwort ein.
- Vergeben Sie beim Erstellen von Benutzerkonten ein zufällig generiertes initiales Kennwort.
  - Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | PAG | Accounts | InitialRandomPassword**.

- Verwenden Sie zielsystemspezifische Kennwortrichtlinien und definieren Sie in den Kennwortrichtlinien die Zeichenklassen, die das Kennwort enthalten muss.
- Legen Sie fest, an welche Person das initiale Kennwort per E-Mail versendet wird.

Verwandte Themen

- Kennwortrichtlinien für PAM Benutzer auf Seite 112
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 125

E-Mail-Benachrichtigungen über Anmeldeinformationen

Die Anmeldeinformationen für neue Benutzerkonten können per E-Mail an eine festgelegte Person gesendet werden. Dabei werden zwei Benachrichtigungen versendet, die den Benutzernamen und das initiale Kennwort enthalten. Zur Erzeugung der Benachrichtigungen werden Mailvorlagen genutzt. In einer Mailvorlage sind die Mailtexte in verschiedenen Sprachen definiert. Somit wird bei Generierung einer E-Mail Benachrichtigung die Sprache des Empfängers berücksichtigt. In der Standardinstallation sind bereits Mailvorlagen enthalten, die Sie zur Konfiguration der Benachrichtigungsverfahren verwenden können.

Um Benachrichtigungen zu nutzen, sind folgende Voraussetzungen zu erfüllen:

- Stellen Sie sicher, dass das E-Mail-Benachrichtungssystem im One Identity Manager konfiguriert ist. Ausführliche Informationen finden Sie im *One Identity Manager Installationshandbuch*.
- Aktivieren Sie im Designer den Konfigurationsparameter **Common | MailNotification | DefaultSender** und geben Sie die Absenderadresse an, mit der die E-Mail Benachrichtigungen verschickt werden.
- Stellen Sie sicher, dass alle Personen eine Standard-E-Mail-Adresse besitzen. An diese E-Mail Adresse werden die Benachrichtigungen versendet. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.
- Stellen Sie sicher, dass für alle Personen eine Sprachkultur ermittelt werden kann. Nur so erhalten die Personen die E-Mail Benachrichtigungen in ihrer Sprache. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Wenn bei der Neuanlage eines Benutzerkontos ein zufällig generiertes initiales Kennwort vergeben wird, werden die initialen Anmeldeinformationen für dieses Benutzerkonto per E-Mail an eine vorher festgelegt Person gesendet.

Um die initialen Anmeldeinformationen per E-Mail zu versenden

1. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | PAG | Accounts | InitialRandomPassword**.
2. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | PAG | Accounts | InitialRandomPassword | SendTo** und erfassen Sie als Wert den Empfänger der Benachrichtigung.

   Ist kein Empfänger ermittelbar, dann wird die E-Mail an die im Konfigurationsparameter **TargetSystem | PAG | DefaultAddress** hinterlegte Adresse versandt.
3. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | PAG | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName**.

   Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Person - Erstellung neues Benutzerkonto** versendet. Die Benachrichtigung enthält den Namen des Benutzerkontos.
4. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | PAG | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword**.

   Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Person - Initiales Kennwort für neues Benutzerkonto** versendet. Die Benachrichtigung enthält das initiale Kennwort für das Benutzerkonto.

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

Abbildung von PAM Objekten im One Identity Manager

Im One Identity Manager werden die Benutzerkonten, Benutzergruppen, Assets, Assetgruppen, Konten, Kontogruppen, Verzeichnisse, Nutzungsrechte und Zugriffsanforderungsrichtlinien eines Privileged Account Management Systems abgebildet. Diese Objekte werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können im Manager angezeigt oder bearbeitet werden.

Detaillierte Informationen zum Thema

- PAM Appliances auf Seite 127
- PAM Benutzerkonten auf Seite 132
- PAM Benutzergruppen auf Seite 149
- PAM Assets auf Seite 154
- PAM Assetgruppen auf Seite 155
- PAM Assetkonten auf Seite 155
- PAM Verzeichniskonten auf Seite 156
- PAM Kontogruppen auf Seite 157
- PAM Verzeichnisse auf Seite 158
- PAM Nutzungsrechte auf Seite 159
- PAM Zugriffsanforderungsrichtlinien auf Seite 160
- Berichte über PAM Objekte auf Seite 160

PAM Appliances

Das Zielsystem der Synchronisation mit One Identity Safeguard ist die Appliance. Appliances werden als Basisobjekte der Synchronisation im One Identity Manager angelegt. Sie werden genutzt, um Provisionierungsprozesse, die automatische Zuordnung

von Personen zu Benutzerkonten und die Vererbung von PAM Benutzergruppen an Benutzerkonten zu konfigurieren.

Detaillierte Informationen zum Thema

- PAM Appliances erstellen auf Seite 128
- Stammdaten von PAM Appliances bearbeiten auf Seite 129
- Allgemeine Stammdaten von PAM Appliances auf Seite 129
- Kategorien für die Vererbung von PAM Benutzergruppen definieren auf Seite 131
- Überblick über eine PAM Appliance
- Synchronisationsprojekt für eine PAM Appliance bearbeiten auf Seite 132
- Suchkriterien für die automatische Personenzuordnung bearbeiten
- Einzelobjekte synchronisieren auf Seite 47

PAM Appliances erstellen

HINWEIS: Die Einrichtung der Appliances in der One Identity Manager-Datenbank übernimmt der Synchronization Editor. Falls erforderlich, können Appliances auch im Manager erstellt werden.

Um eine Appliance einzurichten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten für die Appliance.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von PAM Appliances bearbeiten auf Seite 129
- Allgemeine Stammdaten von PAM Appliances auf Seite 129
- Kategorien für die Vererbung von PAM Benutzergruppen definieren auf Seite 131

Stammdaten von PAM Appliances bearbeiten

Um die Stammdaten einer Appliance zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances**.
2. Wählen Sie in der Ergebnisliste die Appliance.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für die Appliance.
5. Speichern Sie die Änderungen.

Verwandte Themen

- PAM Appliances erstellen auf Seite 128
- Allgemeine Stammdaten von PAM Appliances auf Seite 129
- Kategorien für die Vererbung von PAM Benutzergruppen definieren auf Seite 131

Allgemeine Stammdaten von PAM Appliances

Auf dem Tabreiter **Allgemein** erfassen Sie die folgenden Stammdaten.

Tabelle 20: Allgemeine Stammdaten eines Appliance

Eigenschaft	Beschreibung
Appliance	Name der Appliance.
URL	Adresse (URL) der PAM Webanwendung. Diese Adresse wird benötigt, damit sich PAM Benutzer über das Web Portal am PAM System anmelden können, um beispielsweise ein angefordertes Kennwort abzuholen oder eine angeforderte Sitzung zu starten.
Modell	Modellbezeichnung der Appliance.
Applianceversion	Versionsnummer der Appliance.
Netzwerkschnittstelle X0	IP-Adresse der primären Schnittstelle der Appliance im IPv4 oder IPv6 Format.
Netzwerkschnittstelle X01	IP-Adresse für das Sitzungsmodul im IPv4 oder IPv6 Format.
Geclustert	Angabe, ob die Appliance geclustert ist.

Eigenschaft	Beschreibung
Kontendefinition (initial)	Initiale Kontendefinition zur Erzeugung von Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für diese Appliance die automatische Zuordnung von Personen zu Benutzerkonten genutzt wird und dabei bereits verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen sollen. Es wird der Standardautomatisierungsgrad der Kontendefinition angewendet. Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen Synchronisation der Fall.
Zielsystemverantwortliche	Anwendungsrolle, in der die Zielsystemverantwortlichen der Appliance festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte der Appliance, der sie zugeordnet sind. Jeder Appliance können andere Zielsystemverantwortliche zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle aus, deren Mitglieder verantwortlich für die Administration dieser Appliance sind. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.
Synchronisiert durch	Art der Synchronisation, über welche die Daten zwischen der Appliance und dem One Identity Manager ausgetauscht werden. Sobald Objekte für diese Appliance im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden. Beim Erstellen einer Appliance mit dem Synchronization Editor wird **One Identity Manager** verwendet.

Tabelle 21: Zulässige Werte

Wert	Synchronisation durch	Provisionierung durch
One Identity Manager	One Identity Safeguard Konnektor	One Identity Safeguard Konnektor
Keine Synchronisation	keine	keine

HINWEIS: Wenn Sie **Keine Synchronisation** festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.

Verwandte Themen

- Kontendefinitionen an PAM Appliances zuweisen auf Seite 75
- Automatische Zuordnung von Personen zu PAM Benutzerkonten auf Seite 79
- Zielsystemverantwortliche für PAM Systeme auf Seite 175

Kategorien für die Vererbung von PAM Benutzergruppen definieren

Im One Identity Manager können Benutzergruppen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Benutzergruppen und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält zwei Tabellen; die Benutzerkontentabelle und die Gruppentabelle. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In der Gruppentabelle geben Sie Ihre Kategorien für die zielsystemabhängigen Gruppen an. In den übrigen Tabellen geben Sie Ihre Kategorien für die Benutzergruppen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 63**.

Um Kategorien zu definieren

1. Wählen Sie im Manager in der Kategorie **Privileged Account Management > Appliances** die Appliance.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wechseln Sie auf den Tabreiter **Abbildungsvorschrift Kategorien**.
4. Erweitern Sie den jeweiligen Basisknoten der Benutzerkontentabelle bzw. der Gruppentabelle.
5. Aktivieren Sie die Kategorie per Maus-Doppelklick auf das Symbol .
6. Tragen Sie eine beliebige Benennung der Kategorie für Benutzerkonten und Gruppen in der verwendeten Anmeldesprache ein.
7. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Vererbung von PAM Benutzergruppen anhand von Kategorien auf Seite 108

Synchronisationsprojekt für eine PAM Appliance bearbeiten

Synchronisationsprojekte, in denen eine Appliance bereits als Basisobjekt verwendet wird, können auch über den Manager geöffnet werden. In diesem Modus können beispielsweise die Konfigurationseinstellungen überprüft oder die Synchronisationsprotokolle eingesehen werden. Der Synchronization Editor wird nicht mit seinem vollen Funktionsumfang gestartet. Verschiedene Funktionen, wie Simulieren oder Ausführen einer Synchronisation, Starten des Zielsystembrowsers und andere, können nicht ausgeführt werden.

HINWEIS: Der Manager ist währenddessen für die Bearbeitung gesperrt. Um Objekte im Manager bearbeiten zu können, schließen Sie den Synchronization Editor.

Um ein bestehendes Synchronisationsprojekt im Synchronization Editor zu öffnen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances**.
2. Wählen Sie in der Ergebnisliste die Appliance.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten**.

Verwandte Themen

- Anpassen der Synchronisationskonfiguration für One Identity Safeguard auf Seite 33

Überblick über PAM Appliances anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Appliance.

Um einen Überblick über eine Appliance zu erhalten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances**.
2. Wählen Sie in der Ergebnisliste die Appliance.
3. Wählen Sie die Aufgabe **Überblick über die PAM Appliance**.

PAM Benutzerkonten

Mit dem One Identity Manager verwalten Sie die Benutzerkonten eines Privileged Account Management Systems. Mit einem Benutzerkonto kann sich eine Person am Privileged

Account Management System, beispielsweise an One Identity Safeguard anmelden. One Identity Manager verwaltet die lokalen Benutzer eines Privileged Account Management Systems und Verzeichnisbenutzer. Verzeichnisbenutzer sind Benutzerkonten aus einem externen Zielsystem wie beispielsweise Active Directory oder LDAP.

Über seine Benutzergruppen erhält ein Benutzerkonto die erforderlichen Nutzungsrechte, um beispielsweise ein Kennwort für einen Assetkonto oder eine Sitzung für die Konten und Assets im Privileged Account Management System anfordern zu können.

Ein Benutzerkonto kann im One Identity Manager mit einer Person verbunden sein. Ebenso können Sie die Benutzerkonten getrennt von Personen verwalten.

HINWEIS: Um Benutzerkonten für die Personen eines Unternehmens einzurichten, wird der Einsatz von Kontendefinitionen empfohlen. Einige der nachfolgend beschriebenen Stammdaten werden dabei über Bildungsregeln aus den Personenstammdaten gebildet.

HINWEIS: Sollen Personen ihre Benutzerkonten über Kontendefinitionen erhalten, müssen die Personen ein zentrales Benutzerkonto besitzen und über die Zuordnung zu einer primären Abteilung, einem primären Standort oder einer primären Kostenstelle ihre IT Betriebsdaten erhalten.

Verwandte Themen

- Managen von PAM Benutzerkonten und Personen auf Seite 56
- Managen von Zuweisungen von PAM Benutzergruppen auf Seite 94
- Kontendefinitionen für PAM Benutzerkonten auf Seite 57
- Lokale PAM Benutzerkonten erstellen auf Seite 134
- Zertifikatsbasierte PAM Benutzerkonten erstellen auf Seite 134
- PAM Benutzerkonten für Verzeichnisbenutzer erstellen auf Seite 135
- Stammdaten für PAM Benutzerkonten bearbeiten auf Seite 137
- Allgemeine Stammdaten für PAM Benutzerkonten auf Seite 138
- Kontaktinformationen für PAM Benutzerkonten auf Seite 143
- Sekundäre Authentifizierung für PAM Benutzerkonten auf Seite 144
- Administrative Berechtigungen für PAM Benutzerkonten auf Seite 145
- Zusatzeigenschaften an PAM Benutzerkonten zuweisen auf Seite 146
- PAM Benutzerkonten deaktivieren auf Seite 147
- PAM Benutzerkonten löschen und wiederherstellen auf Seite 148
- Überblick über PAM Benutzerkonten anzeigen auf Seite 149
- Einzelobjekte synchronisieren auf Seite 47

Lokale PAM Benutzerkonten erstellen

Um ein lokales PAM Benutzerkonto zu erstellen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Tabreiter **Allgemein** erfassen Sie mindestens die folgenden Informationen:
    - **Appliance**: Appliance, zu der das Benutzerkonto gehört.
    - **Identitätsanbieter**: Wählen Sie den Wert **Local**.
    - **Benutzername**: Erfassen Sie den Namen zur Anzeige.
    - **Authentifizierungsanbieter**: Wählen Sie, wie sich der Benutzer am Privileged Account Management System authentifiziert. Abhängig vom Authentifizierungsanbieter sind weitere Eingaben erforderlich.
        - **Local**: Erfassen Sie den Anmeldenamen, das Kennwort und die Kennwortbestätigung.
        - **<Externer Verbund>**: Erfassen Sie die E-Mail-Adresse oder den Namensanspruch.
        - **<RADIUS-Server>**: Erfassen Sie den Anmeldenamen auf dem RADIUS-Server.
    - **Zeitzone**: Zeitzone des Benutzers. Die Standardzeitzone ist **UTC** (Coordinated Universal Time).
4. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für PAM Benutzerkonten auf Seite 138
- Kontaktinformationen für PAM Benutzerkonten auf Seite 143
- Sekundäre Authentifizierung für PAM Benutzerkonten auf Seite 144
- Administrative Berechtigungen für PAM Benutzerkonten auf Seite 145
- Stammdaten für PAM Benutzerkonten bearbeiten auf Seite 137
- Zertifikatsbasierte PAM Benutzerkonten erstellen auf Seite 134
- PAM Benutzerkonten für Verzeichnisbenutzer erstellen auf Seite 135

Zertifikatsbasierte PAM Benutzerkonten erstellen

Die Benutzer eines zertifikatsbasierten PAM Benutzerkontos authentifizieren sich über ein Zertifikat am Privileged Account Management System.

Um ein zertifikatsbasiertes PAM Benutzerkonto zu erstellen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Tabreiter **Allgemein** erfassen Sie mindestens die folgenden Informationen:
    - **Appliance**: Appliance, zu der das Benutzerkonto gehört.
    - **Identitätsanbieter**: Wählen Sie den Wert **Local**.
    - **Benutzername**: Erfassen Sie den Namen zur Anzeige.
    - **Authentifizierungsanbieter**: Wählen Sie den Wert **Certificate**.
    - **Zertifikatfingerabdruck (SHA-1)**: Geben Sie den eindeutigen Hash-Wert (40 hexadezimale Zeichen) des Zertifikats ein.

      HINWEIS: Sie können den Fingerabdruck-Wert direkt aus dem Zertifikat kopieren und einfügen, einschließlich der Leerzeichen.
    - **Zeitzone**: Zeitzone des Benutzers. Die Standardzeitzone ist **UTC** (Coordinated Universal Time).
4. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für PAM Benutzerkonten auf Seite 138
- Kontaktinformationen für PAM Benutzerkonten auf Seite 143
- Sekundäre Authentifizierung für PAM Benutzerkonten auf Seite 144
- Administrative Berechtigungen für PAM Benutzerkonten auf Seite 145
- Stammdaten für PAM Benutzerkonten bearbeiten auf Seite 137
- Lokale PAM Benutzerkonten erstellen auf Seite 134
- PAM Benutzerkonten für Verzeichnisbenutzer erstellen auf Seite 135

PAM Benutzerkonten für Verzeichnisbenutzer erstellen

Verzeichnisbenutzer sind Benutzerkonten aus einem externen Zielsystem wie beispielsweise Active Directory oder LDAP.

Verzeichnisbenutzer können Sie im One Identity Manager nur erstellen, wenn die Active Directory-Umgebung oder die LDAP-Umgebung in den One Identity Manager eingelesen ist.

Um ein PAM Benutzerkonto für Verzeichnisbenutzer zu erstellen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Tabreiter **Allgemein** erfassen Sie mindestens die folgenden Informationen:
   - **Appliance**: Appliance, zu der das Benutzerkonto gehört.
   - **Identitätsanbieter**: Basisdomäne des jeweiligen Verzeichnisdienstes.
   - **Identifizierungsobjekt**: Wählen Sie das Benutzerkonto aus dem Identitätsanbieter.
     a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld und erfassen Sie die folgenden Informationen:
        - **Tabelle**: Tabelle, in welcher die Benutzerkonten abgebildet werden. Die Tabelle ist vorausgewählt.

          Für ein Active Directory Benutzerkonto ist **ADSAccount** ausgewählt. Für ein LDAP Benutzerkonto ist **LDAPAccount** ausgewählt.
        - **Identifizierungsobjekt**: Wählen Sie das Benutzerkonto.

     b. Klicken Sie **OK**.

     Die Domäne, der Benutzername und der Anzeigename werden aus dem Benutzerkonto ermittelt.
   - **Authentifizierungsanbieter**: Wählen Sie, wie sich der Benutzer am Privileged Account Management System authentifiziert. Abhängig vom Authentifizierungsanbieter sind weitere Eingaben erforderlich.
     - **<Verzeichnisname>**: Wählen Sie die Active Directory Domäne oder die LDAP Domäne des Benutzerkontos.

       Für eine Active Directory Domäne können Sie optional festlegen, ob eine Zertifikatsauthentifizierung erforderlich ist. Aktivieren Sie die Option **Zertifikatsauthentifizierung erforderlich** wenn sich der Benutzer nur mit einem domänenausgestellten Benutzerzertifikat oder SmartCard anmelden kann.
     - **<Externer Verbund>**: Erfassen Sie die E-Mail-Adresse oder den Namensanspruch.
     - **<RADIUS-Server>**: Erfassen Sie den Anmeldenamen auf dem RADIUS-Server.
   - **Zeitzone**: Zeitzone des Benutzers. Die Standardzeitzone ist **UTC** (Coordinated Universal Time).
4. Speichern Sie die Änderungen.

HINWEIS: Wenn Sie Kontendefinitionen einsetzen, um PAM Benutzerkonten für Personen zu erstellen, können Sie für eine PAM Appliance optional eine Active Directory Kontendefinition oder eine LDAP Kontendefinition als vorausgesetzte Kontendefinition festlegen. In diesem Fall wird für die Person zunächst ein Active Directory oder LDAP Benutzerkonto

erzeugt. Ist dieses Benutzerkonto vorhanden, wird das PAM Benutzerkonto als Verzeichnisbenutzer erstellt.

Verwandte Themen

- Allgemeine Stammdaten für PAM Benutzerkonten auf Seite 138
- Kontaktinformationen für PAM Benutzerkonten auf Seite 143
- Sekundäre Authentifizierung für PAM Benutzerkonten auf Seite 144
- Administrative Berechtigungen für PAM Benutzerkonten auf Seite 145
- Stammdaten für PAM Benutzerkonten bearbeiten auf Seite 137
- Lokale PAM Benutzerkonten erstellen auf Seite 134
- Zertifikatsbasierte PAM Benutzerkonten erstellen auf Seite 134
- Kontendefinitionen für PAM Benutzerkonten auf Seite 57

Stammdaten für PAM Benutzerkonten bearbeiten

Um die Stammdaten eines Benutzerkontos zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Benutzerkontos.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für PAM Benutzerkonten auf Seite 138
- Kontaktinformationen für PAM Benutzerkonten auf Seite 143
- Sekundäre Authentifizierung für PAM Benutzerkonten auf Seite 144
- Administrative Berechtigungen für PAM Benutzerkonten auf Seite 145
- PAM Benutzerkonten deaktivieren auf Seite 147
- PAM Benutzerkonten löschen und wiederherstellen auf Seite 148

Allgemeine Stammdaten für PAM Benutzerkonten

Auf dem Tabreiter **Allgemein** erfassen Sie die folgenden Stammdaten.

Tabelle 22: Allgemeine Stammdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Appliance	Appliance, zu der das Benutzerkonto gehört.
Person	Person, die das Benutzerkonto verwendet. Wurde das Benutzerkonto über eine Kontendefinition erzeugt, ist die Person bereits eingetragen. Wenn Sie das Benutzerkonto manuell erstellen, können Sie die Person aus der Auswahlliste wählen. Wenn Sie die automatische Personenzuordnung nutzen, wird beim Speichern des Benutzerkontos eine zugehörige Person gesucht und in das Benutzerkonto übernommen. Für ein Benutzerkonto mit einer Identität vom Typ **Organisatorische Identität**, **Persönliche Administratoridentität**, **Zusatzidentität**, **Gruppenidentität** oder **Dienstidentität** können Sie eine neue Person erstellen. Klicken Sie dafür neben dem Eingabefeld und erfassen Sie die erforderlichen Personenstammdaten. Die Pflichteingaben sind abhängig vom gewählten Identitätstyp. HINWEIS: Um mit Identitäten für Benutzerkonten zu arbeiten, benötigen die Personen ebenfalls Identitäten. Benutzerkonten, denen eine Identität zugeordnet ist, können Sie nur mit Personen verbinden, die dieselbe Identität haben.
Keine Verbindung mit einer Person erforderlich	Gibt an, ob dem Benutzerkonto absichtlich keine Person zugeordnet ist. Die Option wird automatisch aktiviert, wenn ein Benutzerkonto in der Ausschlussliste für die automatische Personenzuordnung enthalten ist oder eine entsprechende Attestierung erfolgt ist. Sie können die Option manuell setzen. Aktivieren Sie die Option, falls das Benutzerkonto mit keiner Person verbunden werden muss (beispielsweise, wenn mehrere Personen das Benutzerkonto verwenden). Wenn durch die Attestierung diese Benutzerkonten genehmigt werden, werden diese Benutzerkonten künftig nicht mehr zur Attestierung vorgelegt. Im Web Portal können Benutzerkonten, die nicht mit einer Person verbunden sind, nach verschiedenen Kriterien gefiltert

Eigenschaft	Beschreibung
	werden.
Nicht mit einer Person verbunden	Zeigt an, warum für das Benutzerkonto die Option **Keine Verbindung mit einer Person erforderlich** aktiviert ist. Mögliche Werte sind: • **durch Administrator**: Die Option wurde manuell durch den Administrator aktiviert. • **durch Attestierung**: Das Benutzerkonto wurde attestiert. • **durch Ausschlusskriterium**: Das Benutzerkonto wird aufgrund eines Ausschlusskriteriums nicht mit einer Person verbunden. Das Benutzerkonto ist beispielsweise in der Ausschlussliste für die automatische Personenzuordnung enthalten (Konfigurationsparameter **PersonExcludeList**).
Kontendefinition	Kontendefinition, über die das Benutzerkonto erstellt wurde. Die Kontendefinition wird benutzt, um die Stammdaten des Benutzerkontos automatisch zu befüllen und um einen Automatisierungsgrad für das Benutzerkonto festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Person und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein. HINWEIS: Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden. HINWEIS: Über die Aufgabe **Entferne Kontendefinition** am Benutzerkonto können Sie das Benutzerkonto wieder in den Zustand **Linked** zurücksetzen. Dabei wird die Kontendefinition vom Benutzerkonto und von der Person entfernt. Das Benutzerkonto bleibt über diese Aufgabe erhalten, wird aber nicht mehr über die Kontendefinition verwaltet. Die Aufgabe entfernt nur Kontendefinitionen, die direkt zugewiesen sind (`XOrigin=1`).
Automatisierungsgrad	Automatisierungsgrad des Benutzerkontos. Wählen Sie einen Automatisierungsgrad aus der Auswahlliste. Den Automatisierungsgrad können Sie nur festlegen, wenn Sie auch eine Kontendefinition eingetragen haben. In der Auswahlliste werden alle Automatisierungsgrade der gewählten Kontendefinition angeboten.
Identitätsanbieter	Quelle, aus der die personenbezogenen Daten des Benutzerkontos stammen. Zulässige Werte sind:

Eigenschaft	Beschreibung
	• **Local**: Lokales PAM Benutzerkonto. Für dieses Benutzerkonten können Kontaktinformationen erfasst werden. • **<Verzeichnisname>**: Externer Identitätsanbieter. Basisdomäne des jeweiligen Verzeichnisdienstes, beispielsweise Active Directory oder LDAP. Kontaktinformationen werden aus dem Active Directory Benutzerkonto oder dem LDAP Benutzerkonto ermittelt. Diese Variante ist nur verfügbar, wenn die Active Directory Domäne oder die LDAP Domäne in den One Identity Manager eingelesen ist.
Identifizierungsobjekt	Benutzerkonto im Active Directory oder LDAP.
Authentifizierungsanbieter	Gibt an, wie sich der Benutzer am Privileged Account Management System authentifiziert. Zulässige Werte sind: • **Certificate**: (Nur für lokale Identitätsanbieter) Die Authentifizierung erfolgt über ein Zertifikat. • **Local**: (Nur für lokale Identitätsanbieter) Die Authentifizierung erfolgt über Benutzername und Kennwort. • **<Verzeichnisname>**: (Nur für externe Identitätsanbieter) Domäne des Identifizierungsobjektes. Die Authentifizierung erfolgt über ein Benutzerkonto des jeweiligen Verzeichnisdienstes, beispielsweise Active Directory Benutzerkonto oder LDAP Benutzerkonto. Diese Variante ist nur verfügbar, wenn die Active Directory Domäne oder die LDAP Domäne in den One Identity Manager eingelesen ist. • **<Externer Verbund>**: Name des externen Verbundes. Die angegebene E-Mail-Adresse oder der Namensanspruch wird für die Authentifizierung verwendet. • **<RADIUS Server>**: Name des RADIUS-Servers. Die Authentifizierung erfolgt über den Anmeldenamen auf dem RADIUS-Server.
Benutzername	Benutzername des PAM Benutzerkontos.
Anmeldename	Anmeldename des PAM Benutzerkontos.

Eigenschaft	Beschreibung
Kennwort	Kennwort für das Benutzerkonto. Das zentrale Kennwort der zugeordneten Person kann auf das Kennwort des Benutzerkontos abgebildet werden. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*. Wenn Sie ein zufällig generiertes initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen. Das Kennwort wird nach dem Publizieren in das Zielsystem aus der Datenbank gelöscht. HINWEIS: Beim Prüfen eines Benutzerkennwortes werden die One Identity Manager Kennwortrichtlinien beachtet. Stellen Sie sicher, dass die Kennwortrichtlinie nicht gegen die Anforderungen des Zielsystems verstößt.
Bestätigung	Kennwortwiederholung.
Kennwort läuft nie ab	Gibt an, ob ein Kennwort abläuft. Diese Option wird in der Regel für Dienstkonten verwendet.
Kennwort bei der nächsten Anmeldung ändern	Gibt an, ob der Benutzer bei der nächsten Anmeldung das Kennwort anpassen muss.
Domäne	Domäne der Benutzerkontos.
Zertifikatsauthentifizierung erforderlich	Gibt an, ob der Benutzer sich nur mit einem domänenausgestellten Benutzerzertifikat oder SmartCard anmelden kann.
Zertifikatsfingerabdruck (SHA-1)	Eindeutiger Hash-Wert (40 hexadezimale Zeichen) des Zertifikats.
E-Mail-Adresse oder Namens-anspruch	E-Mail-Adresse oder Namensanspruch des Benutzerkontos im externen Verbund.
Anzeigename	Anzeigename des PAM Benutzerkontos.
Letzte Anmeldung	Zeitpunkt der letzten Anmeldung am System.
Zeitzone	Zeitzone des Benutzers. Die Standardzeitzone ist **UTC** (Coordinated Universal Time).
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten Gruppen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One*

Eigenschaft	Beschreibung
	Identity Manager Administrationshandbuch für Risikobewertungen.
Kategorie	Kategorien für die Vererbung von Gruppen an das Benutzerkonto. Gruppen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Identität	Typ der Identität des Benutzerkontos. Zulässige Werte sind: • **Primäre Identität**: Standardbenutzerkonto einer Person. • **Organisatorische Identität**: Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen. • **Persönliche Administratoridentität**: Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird. • **Zusatzidentität**: Benutzerkonto, das für einen spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken. • **Gruppenidentität**: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird. Weisen Sie alle Personen zu, die das Benutzerkonto nutzen. • **Dienstidentität**: Dienstkonto.
Gruppen erbbar	Gibt an, ob das Benutzerkonto Gruppen über die verbundene Person erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Person Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Person eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto

Eigenschaft	Beschreibung
	der Person diese Gruppe nur, wenn die Option aktiviert ist.
Privilegiertes Benutzerkonto	Gibt an, ob es sich um ein privilegiertes Benutzerkonto handelt.
Systemobjekt	Kennzeichnet den Benutzer als Systembestandteil.
Benutzerkonto ist deaktiviert	Gibt an, ob das Benutzerkonto deaktiviert ist. Wird ein Benutzerkonto vorübergehend nicht benötigt, können Sie das Benutzerkonto über die Option zeitweilig deaktivieren.
Konto gesperrt	Gibt an, ob das Benutzerkonto gesperrt ist. Abhängig von der Konfiguration wird nach mehrmaliger falscher Kennworteingabe das Benutzerkonto im Privileged Account Management System gesperrt.
Angelegt am	Zeitpunkt, an dem das Benutzerkonto erstellt wurde.
Angelegt von	Benutzer, der das Benutzerkonto erstellt hat.

Verwandte Themen

- Managen von PAM Benutzerkonten und Personen auf Seite 56
- Kontendefinitionen für PAM Benutzerkonten auf Seite 57
- Automatische Zuordnung von Personen zu PAM Benutzerkonten auf Seite 79
- Vererbung von PAM Benutzergruppen anhand von Kategorien auf Seite 108
- Voraussetzungen für indirekte Zuweisungen von PAM Gruppen an PAM Benutzerkonten auf Seite 96
- PAM Benutzerkonten deaktivieren auf Seite 147
- Unterstützte Typen von Benutzerkonten auf Seite 86

Kontaktinformationen für PAM Benutzerkonten

Auf dem Tabreiter **Kontaktinformationen** erfassen Sie die folgenden Stammdaten. Kontaktinformationen können nur für Benutzerkonten erfasst werden, die einen lokalen Identitätsanbieter verwenden.

Tabelle 23: Kontaktinformationen eines Benutzerkontos

Eigenschaft	Beschreibung
Vorname	Vorname des Benutzers. Haben Sie eine Kontendefinition zugeordnet,

Eigenschaft	Beschreibung
	wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Nachname	Nachname des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Telefon	Telefonnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Mobiltelefon	Mobiltelefonnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
E-Mail-Adresse	E-Mail-Adresse des Benutzerkontos. Haben Sie eine Kontendefinition zugeordnet, wird, abhängig vom Automatisierungsgrad, die E-Mail-Adresse aus der Standard-E-Mail-Adresse der Person gebildet.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Sekundäre Authentifizierung für PAM Benutzerkonten

Falls einen Multifaktor-Authentifizierung für den Benutzer erforderlich ist, erfassen Sie auf dem Tabreiter **Sekundäre Authentifizierung** die folgenden Stammdaten.

Tabelle 24: Sekundäre Authentifizierung eines Benutzerkontos

Eigenschaft	Beschreibung
Sekundäre Authentifizierung	Zweiter Authentifizierungsanbieter um den Benutzer zu einer Multifaktor-Authentifizierung aufzufordern. Es werden alle Authentifizierungsanbieter angezeigt, die als sekundärer Authentifizierungsanbieter erlaubt sind (Tabelle `PAGAuthProvider`, Spalte `AllowSecondaryAuth`).
Sekundäres Authentifizierungsobjekt	(Nur für Verzeichnisbenutzer) Zeichenkette zur Identifizierung des zweiten Authentifizierungsobjektes für die Multifaktor-Authentifizierung. Die Eingabe ist abhängig vom gewählten sekundären Authentifizierungsanbieter. Erfolgt die sekundäre Authentifizierung des Benutzers über ein Active Directory Benutzerkonto oder ein LDAP Benutzerkonto, können Sie das Benutzerkonto auswählen. ***Um ein Benutzerkonto auszuwählen***

Eigenschaft	Beschreibung
	1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld und erfassen Sie die folgenden Informationen: • **Tabelle**: Tabelle, in welcher die Benutzerkonten abgebildet werden. Die Tabelle ist vorausgewählt. Für ein Active Directory Benutzerkonto ist **ADSAccount** ausgewählt. Für ein LDAP Benutzerkonto ist **LDAPAccount** ausgewählt • **Sekundäres Authentifizierungsobjekt**: Wählen Sie das Benutzerkonto. 2. Klicken Sie **OK**.
Anmeldename	Anmeldename des PAM Benutzerkontos für die sekundäre Authentifizierung.

Administrative Berechtigungen für PAM Benutzerkonten

Falls erforderlich, legen Sie auf dem Tabreiter **Berechtigungen** die administrativen Berechtigungen des Benutzers fest. Ausführliche Informationen zu administrativen Berechtigungen in One Identity Safeguard finden Sie im *One Identity Safeguard Administration Guide*.

Tabelle 25: Administrative Berechtigungen eines Benutzerkontos

Administrative Rolle	Beschreibung
Autorisierer	Erlaubt dem Benutzer, anderen Benutzern Berechtigungen zu erteilen.
Benutzer	Erlaubt dem Benutzer, neue Benutzer zu erstellen, Kennwörter für nicht-administrative Benutzer freizuschalten und zurückzusetzen.
Help Desk	Erlaubt dem Benutzer, Kennwörter für nicht-administrative Benutzer freizuschalten und festzulegen.
Appliance	Erlaubt dem Benutzer, die Appliance zu bearbeiten, zu aktualisieren und zu konfigurieren.
Vorgänge	Erlaubt dem Benutzer, die Appliance neu zu starten und zu überwachen.

Administrative Rolle	Beschreibung
Auditor	Erlaubt dem Benutzer einen schreibgeschützten Zugriff.
Asset	Erlaubt dem Benutzer das Hinzufügen, Bearbeiten und Löschen von Partitionen, Assets und Konten.
Verzeichnis	Erlaubt dem Benutzer das Hinzufügen, Bearbeiten und Löschen von Verzeichnissen.
Sicherheitsrichtlinie	Erlaubt dem Benutzer das Hinzufügen, Bearbeiten und Löschen von Berechtigungen und Richtlinien, die den Zugriff auf Konten und Assets steuern.
Vault für persönliche Kennwörter	Erlaubt dem Benutzer einen Vault für persönliche Kennwörter hinzuzufügen, zu bearbeiten, zu löschen, freizugeben und darauf zuzugreifen.

Verwandte Themen

- Administrative Berechtigungen für PAM Benutzergruppen auf Seite 152

Zusatzeigenschaften an PAM Benutzerkonten zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

Ausführliche Informationen zum Verwenden von Zusatzeigenschaften finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

PAM Benutzerkonten deaktivieren

Wie Sie Benutzerkonten deaktivieren, ist abhängig von der Art der Verwaltung der Benutzerkonten.

Szenario: Die Benutzerkonten sind mit Personen verbunden und werden über Kontendefinitionen verwaltet.

Benutzerkonten, die über Kontendefinitionen verwaltet werden, werden deaktiviert, wenn die Person dauerhaft oder zeitweilig deaktiviert wird. Das Verhalten ist abhängig vom Automatisierungsgrad des Benutzerkontos. Benutzerkonten mit dem Automatisierungsgrad **Full managed** werden entsprechend der Einstellungen an der Kontendefinition deaktiviert. Für Benutzerkonten mit einem anderen Automatisierungsgrad konfigurieren Sie das gewünschte Verhalten an der Bildungsregel der Spalte `PAGUser.IsDisabled`.

Szenario: Die Benutzerkonten sind mit Personen verbunden. Es sind keine Kontendefinitionen zugeordnet.

Benutzerkonten, die mit Personen verbunden sind, jedoch nicht über Kontendefinitionen verwaltet werden, werden deaktiviert, wenn die Person dauerhaft oder zeitweilig deaktiviert wird. Das Verhalten ist abhängig vom Konfigurationsparameter **QER | Person | TemporaryDeactivation**.

- Ist der Konfigurationsparameter aktiviert, werden die Benutzerkonten einer Person deaktiviert, wenn die Person zeitweilig oder dauerhaft deaktiviert wird.
- Ist der Konfigurationsparameter deaktiviert, haben die Eigenschaften der Person keinen Einfluss auf die verbundenen Benutzerkonten.

Um das Benutzerkonto bei deaktiviertem Konfigurationsparameter zu deaktivieren

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Benutzerkonto ist deaktiviert**.
5. Speichern Sie die Änderungen.

Szenario: Die Benutzerkonten sind nicht mit Personen verbunden.

Um ein Benutzerkonto zu deaktivieren, das nicht mit einer Person verbunden ist

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Benutzerkonto ist deaktiviert**.
5. Speichern Sie die Änderungen.

Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Kontendefinitionen für PAM Benutzerkonten auf Seite 57
- Automatisierungsgrade erstellen auf Seite 63
- PAM Benutzerkonten löschen und wiederherstellen auf Seite 148

PAM Benutzerkonten löschen und wiederherstellen

HINWEIS: Solange eine Kontendefinition für eine Person wirksam ist, behält die Person ihr daraus entstandenes Benutzerkonto. Wird die Zuweisung einer Kontendefinition entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht.

Ein Benutzerkonto, das nicht über eine Kontendefinition entstanden ist, löschen Sie über die Ergebnisliste oder über die Menüleiste. Nach Bestätigung der Sicherheitsabfrage wird das Benutzerkonto im One Identity Manager zunächst zum Löschen markiert. Das Benutzerkonto wird im One Identity Manager gesperrt und je nach Einstellung der Löschverzögerung endgültig aus der One Identity Manager-Datenbank und aus dem Zielsystem gelöscht.

Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Um ein Benutzerkonto zu löschen, das nicht über eine Kontendefinition verwaltet wird

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Um ein Benutzerkonto wiederherzustellen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste .

Verwandte Themen

- PAM Benutzerkonten deaktivieren auf Seite 147
- Löschverzögerung für PAM Benutzerkonten festlegen auf Seite 92

Überblick über PAM Benutzerkonten anzeigen

Für ein Benutzerkonto erhalten Sie einen Überblick über die Benutzergruppen und Nutzungsrechte, die mit dem Benutzerkonto verbunden sind. Für Verzeichnisbenutzer wird das verbundene Active Directory Benutzerkonto oder LDAP Benutzerkonto angezeigt.

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das PAM Benutzerkonto**.

PAM Benutzergruppen

Über seine Benutzergruppen erhält ein Benutzerkonto die erforderlichen Nutzungsrechte, um beispielsweise ein Kennwort für einen Assetkonto oder eine Sitzung für die Konten und Assets im Privileged Account Management System anfordern zu können.

Bei der Synchronisation werden alle lokalen Benutzergruppen und Verzeichnisgruppen einer Appliance in den One Identity Manager eingelesen. Benutzergruppen sind im One

Identity Manager nur begrenzt bearbeitbar. Sie können beispielsweise lokale Benutzergruppen für die Verwendung im IT Shop anpassen und Benutzerkonten zuweisen.

Verwandte Themen

- Stammdaten für PAM Benutzergruppen bearbeiten auf Seite 150
- Allgemeine Stammdaten für PAM Benutzergruppen auf Seite 150
- Administrative Berechtigungen für PAM Benutzergruppen auf Seite 152
- Zusatzeigenschaften an PAM Benutzergruppen zuweisen auf Seite 153
- Überblick über PAM Benutzergruppen anzeigen auf Seite 154
- Managen von Zuweisungen von PAM Benutzergruppen auf Seite 94
- Einzelobjekte synchronisieren auf Seite 47

Stammdaten für PAM Benutzergruppen bearbeiten

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzergruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für PAM Benutzergruppen auf Seite 150
- Administrative Berechtigungen für PAM Benutzergruppen auf Seite 152

Allgemeine Stammdaten für PAM Benutzergruppen

Auf dem Tabreiter **Allgemein** bearbeiten Sie die folgenden Stammdaten.

Tabelle 26: Allgemeine Stammdaten einer Benutzergruppe

Eigenschaft	Beschreibung
Bezeichnung	Bezeichnung der Benutzergruppe.
Appliance	Appliance, zu der die Benutzergruppe gehört.
Leistungsposition	Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
IT Shop	Gibt an, ob die Gruppe über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Benutzerkonten. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen. Gruppen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Authentifizierungsanbieter	(Nur für Verzeichnisgruppen) Verzeichnisname.
Zielsystemgruppe	(Nur für Verzeichnisgruppen) Gruppe im Active Directory oder LDAP.
Mitgliedschaften schreibgeschützt	(Nur für Verzeichnisgruppen) Die Verzeichnisgruppe ist schreibgeschützt. Die Mitgliedschaften werden im Verzeichnis gepflegt, beispielsweise im Active Directory oder LDAP.
Angelegt am	Zeitpunkt, an dem das Benutzerkonto erstellt wurde.
Angelegt von	Benutzer, der das Benutzerkonto erstellt hat.

Verwandte Themen

- Vererbung von PAM Benutzergruppen anhand von Kategorien auf Seite 108
- Voraussetzungen für indirekte Zuweisungen von PAM Gruppen an PAM Benutzerkonten auf Seite 96
- PAM Benutzergruppen in den IT Shop aufnehmen auf Seite 100
- Lokale PAM Benutzergruppen automatisch in den IT Shop aufnehmen auf Seite 102

Administrative Berechtigungen für PAM Benutzergruppen

Falls erforderlich, legen Sie auf dem Tabreiter **Berechtigungen** die administrativen Berechtigungen der Benutzergruppe fest. Die Berechtigungen gelten für die Benutzer der Benutzergruppe.

Administrative Berechtigungen für PAM Benutzergruppen werden ab One Identity Safeguard 7.0 unterstützt. Ausführliche Informationen zu administrativen Berechtigungen in One Identity Safeguard finden Sie im *One Identity Safeguard Administration Guide*.

Tabelle 27: Administrative Berechtigungen einer Benutzergruppe

Administrative Rolle	Beschreibung
Autorisierer	Erlaubt den Benutzern der Gruppe, anderen Benutzern Berechtigungen zu erteilen.
Benutzer	Erlaubt den Benutzern der Gruppe, neue Benutzer zu erstellen, Kennwörter für nicht-administrative Benutzer freizuschalten und zurückzusetzen.
Help Desk	Erlaubt den Benutzern der Gruppe, Kennwörter für nicht-administrative Benutzer freizuschalten und festzulegen.
Appliance	Erlaubt den Benutzern der Gruppe, die Appliance zu bearbeiten, zu aktualisieren und zu konfigurieren.
Vorgänge	Erlaubt den Benutzern der Gruppe, die Appliance neu zu starten und zu überwachen.
Auditor	Erlaubt den Benutzern der Gruppe einen schreibgeschützten Zugriff.
Asset	Erlaubt den Benutzern der Gruppe das Hinzufügen, Bearbeiten und Löschen von Partitionen, Assets und Konten.
Verzeichnis	Erlaubt den Benutzern der Gruppe das Hinzufügen, Bearbeiten und Löschen von Verzeichnissen.

Administrative Rolle	Beschreibung
Sicherheitsrichtlinie	Erlaubt den Benutzern der Gruppe das Hinzufügen, Bearbeiten und Löschen von Berechtigungen und Richtlinien, die den Zugriff auf Konten und Assets steuern.
Vault für persönliche Kennwörter	Erlaubt den Benutzern der Gruppe einen Vault für persönliche Kennwörter hinzuzufügen, zu bearbeiten, zu löschen, freizugeben und darauf zuzugreifen.

Verwandte Themen

- Administrative Berechtigungen für PAM Benutzerkonten auf Seite 145

Zusatzeigenschaften an PAM Benutzergruppen zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

Ausführliche Informationen zur Einrichtung von Zusatzeigenschaften finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Um Zusatzeigenschaften für eine Gruppe festzulegen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Benutzergruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

Überblick über PAM Benutzergruppen anzeigen

Für eine Benutzergruppe erhalten Sie einen Überblick über die Benutzerkonten und Nutzungsrechte, die mit der Benutzergruppe verbunden sind. Für Verzeichnisgruppen wird die verbundene Active Directory Gruppe oder LDAP Gruppe angezeigt.

Um einen Überblick über eine Gruppe zu erhalten

1. Wählen Sie die Kategorie **Privileged Account Management > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die PAM Benutzergruppe**.

PAM Assets

Assets sind Computer, Server, Netzwerkgeräte oder Anwendungen, die von einer PAM Appliance verwaltet werden.

Assets werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Über die Einzelobjektsynchronisation können Änderungen an den Objekteigenschaften einzelner Assets erneut eingelesen werden.

Um die Eigenschaften eines Assets anzuzeigen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Privilegierte Objekte > Assets**.
2. Wählen Sie in der Ergebnisliste das Asset.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Für ein Asset erhalten Sie einen Überblick über die Assetgruppen, die Assetkonten und die Zugriffsanforderungsrichtlinien, die mit dem Asset verbunden sind.

Um einen Überblick über ein Asset zu erhalten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Privilegierte Objekte > Assets**.
2. Wählen Sie in der Ergebnisliste das Asset.
3. Wählen Sie die Aufgabe **Überblick über das PAM Asset**.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 47
- Eigentümer von PAM Objekten auf Seite 167

PAM Assetgruppen

Eine Assetgruppe ist eine Zusammenfassung von Assets. Eine Assetgruppe kann zum Bereich einer Zugriffsanforderungsrichtlinie hinzugefügt werden.

Assetgruppen werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Die Eigenschaften von Assetgruppen können nicht bearbeitet werden. Über die Einzelobjektsynchronisation können Änderungen an den Objekteigenschaften einzelner Assetgruppen erneut eingelesen werden.

Um die Eigenschaften einer Assetgruppe anzuzeigen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Privilegierte Objekte > Assetgruppen**.
2. Wählen Sie in der Ergebnisliste die Assetgruppe.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Für eine Assetgruppe erhalten Sie einen Überblick über die Assets und die Zugriffsanforderungsrichtlinien, die mit der Assetgruppe verbunden sind.

Um einen Überblick über eine Assetgruppe zu erhalten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Privilegierte Objekte > Assetgruppen**.
2. Wählen Sie in der Ergebnisliste die Assetgruppe.
3. Wählen Sie die Aufgabe **Überblick über die PAM Assetgruppe**.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 47
- Eigentümer von PAM Objekten auf Seite 167

PAM Assetkonten

Ein Assetkonto ist eine eindeutige Kennung für den Zugriff auf ein Asset, beispielsweise ein Benutzerkonto, eine Gruppe oder ein Dienstkonto. Für Assetkonten können Kennworte angefordert werden, um auf die Assets zuzugreifen.

Assetkonten werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Über die Einzelobjektsynchronisation können Änderungen an den Objekteigenschaften einzelner Assetkonten erneut eingelesen werden.

Um einen Überblick über ein Assetkonto zu erhalten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Privilegierte Objekte > Assetkonten**.
2. Wählen Sie in der Ergebnisliste das Assetkonto.
3. Wählen Sie die Aufgabe **Überblick über das PAM Assetkonto**.

Um die Eigenschaften eines Assetkontos anzuzeigen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Privilegierte Objekte > Assetkonten**.
2. Wählen Sie in der Ergebnisliste das Assetkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Für ein Assetkonto erhalten Sie einen Überblick über die Kontengruppen und die Zugriffsanforderungsrichtlinien, die mit dem Assetkonto verbunden sind.

Um einen Risikoindex für ein Assetkonto festzulegen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Privilegierte Objekte > Assetkonten**.
2. Wählen Sie in der Ergebnisliste das Assetkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Stellen Sie für den **Risikoindex** einen Wert zwischen **0** und **1** ein.

   Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 47
- Eigentümer von PAM Objekten auf Seite 167

PAM Verzeichniskonten

Verzeichniskonten sind privilegierte Benutzerkonten in einem Verzeichnis, beispielsweise Active Directory oder LDAP, für die ein Kennwort angefordert werden kann.

Verzeichniskonten werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Über die Einzelobjektsynchronisation können Änderungen an den Objekteigenschaften einzelner Verzeichniskonten erneut eingelesen werden.

Um einen Überblick über ein Verzeichniskonto zu erhalten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Privilegierte Objekte > Verzeichniskonten**.
2. Wählen Sie in der Ergebnisliste das Verzeichniskonto.
3. Wählen Sie die Aufgabe **Überblick über das PAM Verzeichniskonto**.

Um die Eigenschaften eines Verzeichniskontos anzuzeigen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Privilegierte Objekte > Verzeichniskonten**.
2. Wählen Sie in der Ergebnisliste das Verzeichniskonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Für ein Verzeichniskonto erhalten Sie einen Überblick über das Benutzerkonto im Verzeichnis, die PAM Benutzerkonten und die Zugriffsanforderungsrichtlinien, die mit dem Verzeichniskonto verbunden sind.

Um einen Risikoindex für ein Verzeichniskonto festzulegen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Privilegierte Objekte > Verzeichniskonten**.
2. Wählen Sie in der Ergebnisliste das Verzeichniskonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Stellen Sie für den **Risikoindex** einen Wert zwischen **0** und **1** ein.

   Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 47
- Eigentümer von PAM Objekten auf Seite 167

PAM Kontogruppen

Eine Kontogruppe ist eine Zusammenfassung von Assetkonten und Verzeichniskonten. Eine Kontogruppe kann zum Bereich einer Zugriffsanforderungsrichtlinie hinzugefügt werden.

Kontogruppen werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Die Eigenschaften von Kontogruppen können nicht bearbeitet werden. Über die Einzelobjektsynchronisation können Änderungen an den Objekteigenschaften einzelner Kontogruppen erneut eingelesen werden.

Um die Eigenschaften einer Kontogruppe anzuzeigen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Privilegierte Objekte > Kontogruppen**.
2. Wählen Sie in der Ergebnisliste die Kontogruppe.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Für eine Kontogruppe erhalten Sie einen Überblick über die Assetkonten, die Verzeichniskonten und die Zugriffsanforderungsrichtlinien, die mit der Kontogruppe verbunden sind.

Um einen Überblick über eine Kontogruppe zu erhalten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Privilegierte Objekte > Kontogruppen**.
2. Wählen Sie in der Ergebnisliste die Kontogruppe.
3. Wählen Sie die Aufgabe **Überblick über die PAM Kontogruppe**.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 47
- Eigentümer von PAM Objekten auf Seite 167

PAM Verzeichnisse

Verzeichnisse bilden externe Zielsysteme ab, wie beispielsweise Active Directory oder LDAP. Wenn die Active Directory-Umgebung oder die LDAP-Umgebung in den One Identity Manager eingelesen ist, können Sie im One Identity Manager Verzeichnisbenutzer erstellen. Verzeichnisbenutzer und Verzeichnisgruppen werden mit den jeweiligen Active Directory Objekten und LDAP Objekten verbunden.

Verzeichnisse werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Die Eigenschaften von Verzeichnissen können nicht bearbeitet werden. Über die Einzelobjektsynchronisation können Änderungen an den Objekteigenschaften einzelner Verzeichnisse erneut eingelesen werden.

Um die Eigenschaften eines Verzeichnisses anzuzeigen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Verzeichnisse**.
2. Wählen Sie in der Ergebnisliste das Verzeichnis.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Für ein Verzeichnis erhalten Sie einen Überblick über die Benutzerkonten, die Benutzergruppen und die Verzeichniskonten, die mit dem Verzeichnis verbunden sind.

Um einen Überblick über ein Verzeichnis zu erhalten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Verzeichnisse**.
2. Wählen Sie in der Ergebnisliste das Verzeichnis.
3. Wählen Sie die Aufgabe **Überblick über das PAM Verzeichnis**.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 47

PAM Nutzungsrechte

Ein Nutzungsrecht ist ein Set von Zugriffsanforderungsrichtlinien, die den Systemzugriff auf autorisierte Benutzer beschränken. In einem Nutzungsrecht werden in der Regel Berechtigungen, die zum Erfüllen einer Aufgabe benötigt werden, zusammengefasst.

Ein Nutzungsrecht legt fest, welche Benutzer berechtigt sind, Kennwörter für Konten oder Sitzungen für Assets im Rahmen der definierten Zugriffsanforderungsrichtlinien anzufordern.

Nutzungsrechte werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Die Eigenschaften von Nutzungsrechte können nicht bearbeitet werden. Über die Einzelobjektsynchronisation können Änderungen an den Objekteigenschaften einzelner Nutzungsrechte erneut eingelesen werden.

Um die Eigenschaften eines Nutzungsrechts anzuzeigen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Nutzungsrechte**.
2. Wählen Sie in der Ergebnisliste das Nutzungsrecht.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Für ein Nutzungsrecht erhalten Sie einen Überblick über die Benutzerkonten, die Benutzergruppen und die Zugriffsanforderungsrichtlinien, die mit dem Nutzungsrecht verbunden sind.

Um einen Überblick über ein Nutzungsrecht zu erhalten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Nutzungsrechte**.
2. Wählen Sie in der Ergebnisliste das Nutzungsrecht.
3. Wählen Sie die Aufgabe **Überblick über das PAM Nutzungsrecht**.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 47

PAM Zugriffsanforderungsrichtlinien

Eine Zugriffsanforderungsrichtlinien definiert

- den Bereich (das heißt, welche Assets, Assetgruppen , Assetkonten, Verzeichniskonten oder Kontengruppen),
- den Zugriffstyp (Kennwort, SSH, SSH-Schlüssel, Remote-Desktop, Remote-Desktop-Anwendung, Telnet) und
- die Regeln zum Anfordern von Kennwörtern, wie beispielsweise die Dauer oder wie viele Genehmigungen erforderlich sind.

Zugriffsanforderungsrichtlinien werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Über die Einzelobjektsynchronisation können Änderungen an den Objekteigenschaften einzelner Zugriffsanforderungsrichtlinien erneut eingelesen werden.

Um die Eigenschaften einer Zugriffsanforderungsrichtlinie anzuzeigen

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Nutzungsrechte > <Nutzungsrecht>**.
2. Wählen Sie in der Ergebnisliste die Zugriffsanforderungsrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Für einer Zugriffsanforderungsrichtlinie erhalten Sie einen Überblick über den Bereich der Zugriffsanforderungsrichtlinie und die Nutzungsrechte, die mit der Zugriffsanforderungsrichtlinie verbunden sind.

Um einen Überblick über eine Zugriffsanforderungsrichtlinie zu erhalten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Nutzungsrechte > <Nutzungsrecht>**.
2. Wählen Sie in der Ergebnisliste die Zugriffsanforderungsrichtlinie.
3. Wählen Sie die Aufgabe **Überblick über die PAM Zugriffsanforderungsrichtlinie**.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 47
- Konfigurieren der PAM Zugriffsanforderungsrichtlinien auf Seite 171

Berichte über PAM Objekte

Der One Identity Manager stellt verschiedene Berichte zur Verfügung, in denen Informationen über das ausgewählte Basisobjekt und seine Beziehungen zu anderen

Objekten der One Identity Manager-Datenbank aufbereitet sind. Für PAM Systeme stehen folgende Berichte zur Verfügung.

Tabelle 28: Berichte zur Datenqualität eines Zielsystems

Bericht	Bereitgestellt für	Beschreibung
Übersicht anzeigen	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Herkunft)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die Herkunft der zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Historie)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Benutzergruppe	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, welche die ausgewählte Systemberechtigung besitzen.
Übersicht anzeigen	Benutzergruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung und ihre Zuweisungen.
Übersicht anzeigen (inklusive Herkunft)	Benutzergruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung und die Herkunft der zugewiesenen Benutzerkonten.
Übersicht anzeigen (inklusive Historie)	Benutzergruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Abweichende Systemberechtigungen anzeigen	Appliance	Der Bericht enthält alle Systemberechtigungen, die aus manuellen Opera-

Bericht	Bereitgestellt für	Beschreibung
		tionen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager.
Benutzerkonten anzeigen (inklusive Historie)	Appliance	Der Bericht liefert alle Benutzerkonten mit ihren Berechtigungen einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Benutzerkonten mit einer überdurch-schnittliche Anzahl an Systemberechtigungen anzeigen	Appliance	Der Bericht enthält alle Benutzerkonten, die eine überdurchschnittliche Anzahl an Systemberechtigungen besitzen.
Personen mit mehreren Benutzerkonten anzeigen	Appliance	Der Bericht zeigt alle Personen, die mehrere Benutzerkonten besitzen. Der Bericht enthält eine Risikoeinschätzung.
Systemberechtigungen anzeigen (inklusive Historie)	Appliance	Der Bericht zeigt die Systemberechtigungen mit den zugewiesenen Benutzerkonten einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Appliance	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Zielsystem mindestens ein Benutzerkonto besitzen.
Ungenutzte Benut-zerkonten anzeigen	Appliance	Der Bericht enthält alle Benutzerkonten, die in den letzten Monaten nicht verwendet wurden.
Unverbundene Benut-zerkonten anzeigen	Appliance	Der Bericht zeigt alle Benutzerkonten, denen keine Person zugeordnet ist.

Tabelle 29: Zusätzliche Berichte für das Zielsystem

Bericht	Beschreibung
PAM Benutzerkonten- und Gruppenverteilung	Der Bericht enthält eine Zusammenfassung zur Benutzerkonten- und Gruppenverteilung aller PAM Appliances. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager > Übersichten Zielsysteme**.
Datenqualität der PAM Benutzerkonten	Der Bericht enthält verschiedenen Auswertungen zur Datenqualität der Benutzerkonten aller PAM Appliances. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager > Analyse Datenqualität**.
Übersicht über den privilegierten Zugriff der Person	Der Bericht enthält detaillierte Informationen über persönliche und organisatorische Daten sowie die aktuellen privilegierten Zugriffe der Person. Der Bericht wird für Personen angezeigt.

8

PAM Zugriffsanforderungen

Im One Identity Manager können Sie Zugriffsanforderungen für Assets, Assetkonten, Verzeichniskonten, Assetgruppen und Kontogruppen eines PAM Systems bestellen. Für die Bestellung einer Zugriffsanforderung sind im IT Shop die folgenden Produkte vorhanden:

- **Kennwortanforderung**: Zur Anforderung von Kennwörtern für Konten in einem PAM System.
- **SSH-Schlüssel-Anforderung**: Zur Anforderung von SSH-Schlüsseln für Konten in einem PAM System.
- **SSH-Sitzungsanforderung**: Zur Anforderung von SSH-Sitzungen für Assets in einem PAM System.
- **Remote-Desktop-Sitzungsanforderung**: Zur Anforderung von Remote-Desktop-Sitzungen für Assets in einem PAM System.
- **Telnet-Sitzungsanforderung**: Zur Anforderung von Telnet-Sitzungen für Assets in einem PAM System.

Die Bestellung der Zugriffsanforderungen erfolgt im Web Portal. Nach Genehmigung der Bestellung wird im PAM System eine entsprechende Zugriffsanforderung erstellt. Um das angeforderten Kennwort oder die angeforderte Sitzung auszuchecken, meldet sich der Benutzer am PAM System an.

Ausführliche Informationen zur Konfiguration des IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*. Ausführliche Informationen zum Bestellen von Zugriffsanforderungen im Web Portal finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.

Detaillierte Informationen zum Thema

- Systemanforderungen für die Bestellung von PAM Zugriffsanforderungen auf Seite 165
- Bestellen von PAM Zugriffsanforderungen auf Seite 166
- Eigentümer von PAM Objekten auf Seite 167
- Konfigurieren der PAM Zugriffsanforderungsrichtlinien auf Seite 171

Systemanforderungen für die Bestellung von PAM Zugriffsanforderungen

Die Erstellung von Zugriffsanforderungen im PAM System erfolgt über Prozess- und Skriptverarbeitung. Der Jobserver benötigt dieselbe Konfiguration (bezüglich der installierten Software sowie der Berechtigungen und des Zertifikates des Benutzerkontos) wie der Synchronisationsserver. Nutzen Sie den Synchronisationsserver.

Im One Identity Safeguard sind zusätzlich folgenden Systemvoraussetzungen zu gewährleisten:

- Der Anwendung zu Anwendung Dienst (Application-to-Application) ist aktiviert.
- Es wurde eine Anwendung mit folgenden Eigenschaften registriert und aktiviert:
  - **Name**: One Identity Manager
  - **Zertifikatsbenutzer**: Benutzer für den Zugriff auf die One Identity Safeguard Appliance (Synchronisationsbenutzer)
  - **Zugriffsanforderungsbroker**: Aktiviert

    Mindestens ein Benutzer oder eine Benutzergruppe, für die One Identity Safeguard den Zugriff vermitteln soll, muss dem Zugriffsanforderungsbroker zugewiesen sein.

    Die Liste wird bei der Erstellung von Zugriffsanforderungen durch den One Identity Manager aktualisiert.
- Um möglichst immer gültige Zugriffsanforderungen zu erzeugen, sollten an den Nutzungsrechten und an den Zugriffsanforderungsrichtlinien keine Zeiteinschränkungen gesetzt werden.

Ausführliche Informationen zur Einrichtung des Anwendung zu Anwendung Dienstes im One Identity Safeguard und zur Konfiguration der Nutzungsrechte und Zugriffsanforderungsrichtlinien finden Sie im *One Identity Safeguard Administation Guide*.

Verwandte Themen

- Benutzer und Berechtigungen für die Synchronisation mit einer One Identity Safeguard Appliance auf Seite 17
- Einrichten des One Identity Safeguard Synchronisationsservers auf Seite 19

Bestellen von PAM Zugriffsanforderungen

Über die Bestellung der Standardprodukte können Zugriffsanforderungen auf privilegierte Objekte eines PAM Systems erstellt werden. Die Produkte sind mehrfach bestellbare Ressourcen.

Tabelle 30: Standardobjekte für das Bestellen von Zugriffsanforderungen

Produkte:	**Kennwortanforderung**: Zur Anforderung von Kennwörtern für Konten in einem PAM System. **SSH-Schlüssel-Anforderung**: Zur Anforderung von SSH-Schlüsseln für Konten in einem PAM System. **SSH-Sitzungsanforderung**: Zur Anforderung von SSH-Sitzungen für Assets in einem PAM System. **Remote-Desktop-Sitzungsanforderung**: Zur Anforderung von Remote-Desktop-Sitzungen für Assets in einem PAM System. **Telnet-Sitzungsanforderung**: Zur Anforderung von Telnet-Sitzungen für Assets in einem PAM System.
Servicekatagorie:	Privilegierte Zugriffsanforderungen
Regal:	Identity & Access Lifecycle | Privilegierter Zugriff
Entscheidungsverfahren:	PG - Eigentümer der bestellten privilegierten Zugriffsanforderung
Entscheidungsrichtlinie/ Entscheidungsworkflow:	Entscheidung der Bestellungen von privilegierten Zugriffen

Der Besteller übergibt Informationen zur gewünschten Zugriffsanforderung, wie Produkt und Asset oder Konto, auf das zugegriffen werden soll sowie den Zeitraum für den Zugriff. Der Eigentümer des privilegierten Objektes, für das der Zugriff angefordert wird, genehmigt die Bestellung. Im PAM System wird eine entsprechende Zugriffsanforderung erstellt.

In der Bestellung wird vermerkt, ob die Zugriffsanforderung im PAM System erstellt werden konnte und ob die Zugriffsanforderung im PAM System genehmigt wurde. Der Status einer Zugriffsanforderung im PAM System wird zyklisch über den Zeitplan **Auslesen des Status von privilegierten Zugriffsanforderungen** geprüft.

Wurde die Zugriffsanforderung genehmigt, kann sich der Benutzer am PAM System anmelden und das angeforderte Kennwort abholen oder die angeforderte Sitzung starten.

Voraussetzungen

- Das PAM Benutzerkonto des Bestellers besitzt das Nutzungsrecht, um die Zugriffsanforderung zu bestellen.
- In den Zugriffsanforderungsrichtlinien ist die Option **Wirksam für One Identity Manager** aktiviert. Damit können Zugriffsanforderungen für Assets, Assetkonten, Verzeichniskonten, Assetgruppen und Kotntogruppen aus dem Bereich der Zugriffsanforderungsrichtlinie bestellt werden.
- Den bestellbaren Assets, Assetkonten, Verzeichniskonten, Assetgruppen und Kontogruppen ist als Eigentümer eine Anwendungsrolle unter **Privileged Account Governance | Asset- und Konteneigentümer** zugewiesen.
- Den Anwendungsrollen sind Personen zugewiesen.
- Der Zeitplan **Auslesen des Status von privilegierten Zugriffsanforderungen** ist aktiviert. Passen Sie bei Bedarf den Zeitplan im Designer an.
- Die URL der PAM Webanwendung ist an der Appliance eingetragen. Damit können sich die Benutzer aus dem Web Portal heraus am PAMSystem anmelden, um das Kennwort abzuholen oder die Sitzung zu starten.

Ausführliche Informationen zur Konfiguration des IT Shops finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*. Ausführliche Informationen zum Bestellen von Zugriffsanforderungen im Web Portal finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.

Verwandte Themen

- Eigentümer von PAM Objekten auf Seite 167
- Konfigurieren der PAM Zugriffsanforderungsrichtlinien auf Seite 171
- PAM Nutzungsrechte auf Seite 159
- Allgemeine Stammdaten von PAM Appliances auf Seite 129
- Bekannte Probleme bei der Anbindung einer One Identity Safeguard Appliance auf Seite 192

Eigentümer von PAM Objekten

Die Eigentümer privilegierter Objekte wie PAM Assets, PAM Assetkonten, PAM Verzeichniskonten, PAM Assetgruppen und PAM Kontogruppen müssen einer Anwendungsrolle unter der Anwendungsrolle **Privileged Account Governance | Asset- und Konteneigentümer** zugewiesen sein.

Benutzer mit dieser Anwendungsrolle:

- Entscheiden über die Bestellung von Zugriffsanforderungen für privilegierte Objekte.
- Attestieren den möglichen Zugriff von Benutzern auf diese privilegierten Objekte.

Das Entscheidungsverfahren **PG - Eigentümer der bestellten privilegierten Zugriffsanforderung** berücksichtigt die Anwendungsrolle bei der Ermittlung der Entscheider. Das Entscheidungsverfahren **OP - Eigentümer eines privilegierten Objektes** berücksichtigt die Anwendungsrolle bei der Ermittlung der Attestierer.

Ausführliche Informationen zu Genehmigungsverfahren finden Sie im *One Identity Manager Administrationshandbuch für IT Shop* und im *One Identity Manager Administrationshandbuch für Attestierungen*.

Detaillierte Informationen zum Thema

- Automatische Ermittlung der Eigentümer auf Seite 168
- Personen manuell als Eigentümer von PAM Objekten festlegen auf Seite 169
- Anwendungsrollen für Eigentümer von PAM Objekten manuell festlegen auf Seite 170

Automatische Ermittlung der Eigentümer

Die Genehmiger von Zugriffsanforderungsrichtlinien werden initial automatisch die Eigentümer der PAM Assets, PAM Assetkonten, PAM Verzeichniskonten, PAM Assetgruppen und PAM Kontogruppen. Diese Zuordnung erfolgt einmalig, wenn zu einem PAM Objekt eine Zugriffsanforderungsrichtlinie ermittelt werden kann.

- Je Zugriffsanforderungsrichtlinie wird eine neue Anwendungsrolle für die Eigentümer unter der Anwendungsrolle **Privileged Account Governance | Asset- und Konteneigentümer** erstellt.
- Die Genehmiger einer Zugriffsanforderungsrichtlinie werden in die Anwendungsrolle aufgenommen.
- Die Anwendungsrolle wird an die PAM Assets, PAM Assetkonten, PAM Verzeichniskonten, PAM Assetgruppen und PAM Kontogruppen, die im Bereich der Richtlinie liegen, zugewiesen.
- Sind mehrere Zugriffsrichtlinien für ein PAM Objekt definiert, erfolgt die Ermittlung der gültigen Anwendungsrolle über die Nutzungsrechte der Zugriffsanforderungsrichtlinien. Die Eigentümer für ein PAM Objekt werden nach folgender Reihenfolge bestimmt:
    1. Anwendungsrolle der Zugriffsanforderungsrichtlinie, deren Nutzungsrecht die niedrigste Priorität hat
    2. Anwendungsrolle der Zugriffsanforderungsrichtlinie mit der niedrigsten Priorität

HINWEIS:

- Eine Anwendungsrolle für die Eigentümer wird einem PAM Objekt nur automatisch zugewiesen, wenn dem PAM Objekt noch keine Anwendungsrolle zugewiesen ist. Eine bestehende Zuweisung wird nicht geändert.

- Die Eigentümer werden nur initial ermittelt. Änderungen der Genehmiger einer Zugriffsanforderungsrichtlinie werden nicht automatisch in die zugehörige Anwendungsrolle übernommen. Ändern Sie bei Bedarf die Zuordnung der Personen zur Anwendungsrolle manuell.
- Für Zugriffsanforderungsrichtlinien, die im One Identity Safeguard automatisch genehmigt werden, können keine Eigentümer ermittelt werden. In diesem Fall weisen Sie die Personen manuell an die Anwendungsrolle zu.

Verwandte Themen

- Personen manuell als Eigentümer von PAM Objekten festlegen auf Seite 169
- Anwendungsrollen für Eigentümer von PAM Objekten manuell festlegen auf Seite 170

Personen manuell als Eigentümer von PAM Objekten festlegen

Zusätzlich zur automatischen Ermittlung der Eigentümer können Sie die Eigentümer manuell festlegen.

Um Personen manuell als Eigentümer festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie in der Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Asset- und Konteneigentümer** die Anwendungsrolle.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Automatische Ermittlung der Eigentümer auf Seite 168
- Anwendungsrollen für Eigentümer von PAM Objekten manuell festlegen auf Seite 170

Anwendungsrollen für Eigentümer von PAM Objekten manuell festlegen

Bei der automatische Ermittlung der Eigentümer werden Anwendungsrollen erstellt. Sie können weitere Anwendungsrollen manuell festlegen.

Um die Anwendungsrolle für die Eigentümer eines PAM Objektes festzulegen

1. Wählen Sie im Manager in der Kategorie **Privileged Account Management > Appliances > <Appliance> > Privilegierte Objekte** einen der folgenden Filter.
    - Um eine Anwendungsrolle für ein Asset festzulegen, wählen Sie **Assets**.
    - Um eine Anwendungsrolle für eine Assetgruppe festzulegen, wählen Sie **Assetgruppen**.
    - Um eine Anwendungsrolle für ein Assetkonto festzulegen, wählen Sie **Assetkonten**.
    - Um eine Anwendungsrolle für ein Verzeichniskonto festzulegen, wählen Sie **Verzeichniskonten**.
    - Um eine Anwendungsrolle für eine Kontogruppe festzulegen, wählen Sie **Kontogruppen**.
2. Wählen Sie in der Ergebnisliste das PAM Objekt.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Eigentümer (Anwendungsrolle)** die Anwendungsrolle.

    - ODER -

    Klicken Sie neben der Auswahlliste **Eigentümer (Anwendungsrolle)** auf , um eine neue Anwendungsrolle zu erstellen.

    a. Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Privileged Account Governance | Asset- und Konteneigentümer** zu.

    b. Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.
5. Weisen Sie die Personen, die Eigentümer sind, der Anwendungsrolle zu.

Verwandte Themen

- Personen manuell als Eigentümer von PAM Objekten festlegen auf Seite 169
- Automatische Ermittlung der Eigentümer auf Seite 168
- Eigentümer von PAM Objekten auf Seite 167

Konfigurieren der PAM Zugriffsanforderungsrichtlinien

Zugriffsanforderungen für Assets, Assetkonten, Verzeichniskonten, Assetgruppen und Kontogruppen können nur bestellt werden, wenn in der Zugriffsanforderungsrichtlinie die Option **Wirksam für One Identity Manager** aktiviert ist.

Um die Zugriffsanforderungsrichtlinie zu konfigurieren

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Appliances > <Appliance> > Nutzungsrechte > <Nutzungsrecht>**.
2. Wählen Sie in der Ergebnisliste die Zugriffsanforderungsrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Prüfen Sie auf dem Tabreiter **Allgemein** die Option **Wirksam für One Identity Manager**.
    - Ist die Option aktiviert, können Zugriffsanforderungen für Assets, Assetkonten, Verzeichniskonten, Assetgruppen und Kontogruppen aus dem Bereich der Zugriffsanforderungsrichtlinie bestellt werden.
    - Ist die Option nicht aktiviert, ist die Bestellung von Zugriffsanforderungen für Assets, Assetkonten, Verzeichniskonten, Assetgruppen und Kontogruppen aus dem Bereich der Zugriffsanforderungsrichtlinie nicht möglich.

Verwandte Themen

- PAM Zugriffsanforderungsrichtlinien auf Seite 160
- Bestellen von PAM Zugriffsanforderungen auf Seite 166

9

Behandeln von PAM Objekten im Web Portal

Der One Identity Manager bietet seinen Benutzern die Möglichkeit, verschiedene Aufgaben unkompliziert über ein Web Portal zu erledigen.

- Managen von Benutzerkonten und Personen

  Mit der Zuweisung einer Kontendefinition an ein IT Shop Regal kann die Kontendefinition von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Person, beispielsweise einen Manager, wird das Benutzerkonto angelegt.

- Managen von Zuweisungen von Benutzergruppen

  Mit der Zuweisung einer Gruppe an ein IT Shop Regal kann die Gruppe von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Person wird die Gruppe zugewiesen.

  Manager und Administratoren von Organisationen können im Web Portal Gruppen an die Abteilungen, Kostenstellen oder Standorte zuweisen, für die sie verantwortlich sind. Die Gruppen werden an alle Personen vererbt, die Mitglied dieser Abteilungen, Kostenstellen oder Standorte sind.

  Wenn das Geschäftsrollenmodul vorhanden ist, können Manager und Administratoren von Geschäftsrollen im Web Portal Gruppen an die Geschäftsrollen zuweisen, für die sie verantwortlich sind. Die Gruppen werden an alle Personen vererbt, die Mitglied dieser Geschäftsrollen sind.

  Wenn das Systemrollenmodul vorhanden ist, können Verantwortliche von Systemrollen im Web Portal Gruppen an die Systemrollen zuweisen. Die Gruppen werden an alle Personen vererbt, denen diese Systemrollen zugewiesen sind.

- Managen von Zugriffsanforderungen auf privilegierte Objekte

  Über das IT Shop Regal **Identity & Access Lifecycle > Privilegierter Zugriff** können Kennwort- und Sitzungsanforderungen für privilegierte Objekte eine PAM Systems bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Der Eigentümer des privilegierten Objektes, für das der Zugriff angefordert wird, genehmigt die Bestellung. Im PAM System wird eine

entsprechende Zugriffsanforderung erstellt. Konnte die Zugriffsanforderung erfolgreich erstellt werden, kann sich der Benutzer am PAM System anmelden und das angeforderte Kennwort abrufen oder die angeforderte Sitzung starten.

- Attestierung

  Wenn das Modul Attestierung vorhanden ist, kann die Richtigkeit der Eigenschaften von Zielsystemobjekten und von Berechtigungszuweisungen regelmäßig oder auf Anfrage bescheinigt werden. Die Eigentümer privilegierter Objekte attestieren den möglichen Zugriff von Benutzern auf diese privilegierten Objekte. Dafür werden im Manager Attestierungsrichtlinien konfiguriert. Die Attestierer nutzen das Web Portal, um Attestierungsvorgänge zu entscheiden.

- Governance Administration

  Wenn das Modul Complianceregeln vorhanden ist, können Regeln definiert werden, die unzulässige Berechtigungszuweisungen identifizieren und deren Risiken bewerten. Die Regeln werden regelmäßig und bei Änderungen an den Objekten im One Identity Manager überprüft. Complianceregeln werden im Manager definiert. Verantwortliche Personen nutzen das Web Portal, um Regelverletzungen zu überprüfen, aufzulösen und Ausnahmegenehmigungen zu erteilen.

  Wenn das Modul Unternehmensrichtlinien vorhanden ist, können Unternehmensrichtlinien für die im One Identity Manager abgebildeten Zielsystemobjekte definiert und deren Risiken bewertet werden. Unternehmensrichtlinien werden im Manager definiert. Verantwortliche Personen nutzen das Web Portal, um Richtlinienverletzungen zu überprüfen und Ausnahmegenehmigungen zu erteilen.

- Risikobewertung

  Über den Risikoindex von Gruppen kann das Risiko von Gruppenmitgliedschaften für das Unternehmen bewertet werden. Dafür stellt der One Identity Manager Standard-Berechnungsvorschriften bereit. Im Web Portal können die Berechnungsvorschriften modifiziert werden.

- Berichte und Statistiken

  Das Web Portal stellt verschiedene Berichte und Statistiken über die Personen, Benutzerkonten, deren Berechtigungen und Risiken bereit.

Ausführliche Informationen zu den genannten Themen finden Sie unter Managen von PAM Benutzerkonten und Personen auf Seite 56, Zuweisen von PAM Benutzergruppen an PAM Benutzerkonten im One Identity Manager auf Seite 94, PAM Zugriffsanforderungen auf Seite 164 und in folgenden Handbüchern:

- *One Identity Manager Web Designer Web Portal Anwenderhandbuch*
- *One Identity Manager Administrationshandbuch für Attestierungen*
- *One Identity Manager Administrationshandbuch für Complianceregeln*
- *One Identity Manager Administrationshandbuch für Unternehmensrichtlinien*
- *One Identity Manager Administrationshandbuch für Risikobewertungen*

10

Basisdaten für die Verwaltung eines Privileged Account Management Systems

Für die Verwaltung eines Privileged Account Management Systems im One Identity Manager sind folgende Basisdaten relevant.

- Kontendefinitionen

  Um Benutzerkonten automatisch an Personen zu vergeben, kennt der One Identity Manager Kontendefinitionen. Kontendefinitionen können für jedes Zielsystem erzeugt werden. Hat eine Person noch kein Benutzerkonto in einem Zielsystem, wird durch die Zuweisung der Kontendefinition an eine Person ein neues Benutzerkonto erzeugt.

  Weitere Informationen finden Sie unter Kontendefinitionen für PAM Benutzerkonten auf Seite 57.

- Kennwortrichtlinien

  Der One Identity Manager unterstützt Sie beim Erstellen von komplexen Kennwortrichtlinien beispielsweise für Systembenutzerkennwörter, das zentrale Kennwort von Personen sowie für Kennwörter für die einzelnen Zielsysteme. Kennwortrichtlinien werden sowohl bei der Eingabe eines Kennwortes durch den Anwender als auch bei der Generierung von Zufallskennwörtern angewendet.

  In der Standardinstallation werden vordefinierte Kennwortrichtlinien mitgeliefert, die Sie nutzen können und bei Bedarf an Ihre Anforderungen anpassen können. Zusätzlich können Sie eigene Kennwortrichtlinien definieren.

  Weitere Informationen finden Sie unter Kennwortrichtlinien für PAM Benutzer auf Seite 112.

- Zielsystemtypen

  Zielsystemtypen werden für die Konfiguration des Zielsystemabgleichs benötigt. An den Zielsystemtypen werden die Tabellen gepflegt, die ausstehende Objekte enthalten können. Es werden Einstellungen für die Provisionierung von Mitgliedschaften und die Einzelobjektsynchronisation vorgenommen. Zusätzlich dient der Zielsystemtyp zur Abbildung der Objekte im Unified Namespace.

Weitere Informationen finden Sie unter Ausstehende Objekte nachbearbeiten auf Seite 49.

- Zielsystemverantwortliche

  Im One Identity Manager ist eine Standardanwendungsrolle für die Zielsystemverantwortlichen vorhanden. Weisen Sie dieser Anwendungsrolle die Personen zu, die berechtigt sind, alle Appliances im One Identity Manager zu bearbeiten.

  Wenn Sie die Berechtigungen der Zielsystemverantwortlichen auf einzelne Appliances einschränken wollen, definieren Sie weitere Anwendungsrollen. Die Anwendungsrollen müssen der Standardanwendungsrolle untergeordnet sein.

  Weitere Informationen finden Sie unter Zielsystemverantwortliche für PAM Systeme auf Seite 175.

- Server

  Für die Verarbeitung der zielsystemspezifischen Prozesse im One Identity Manager muss der Synchronisationsserver mit seinen Serverfunktionen bekannt sein.

  Weitere Informationen finden Sie unter Jobserver für PAM-spezifische Prozessverarbeitung auf Seite 178.

- Eigentümer privilegierter Objekte

  Im One Identity Manager ist eine Standardanwendungsrolle für die Eigentümer privilegierter Objekte wie PAM Assets, PAM Assetkonten oder PAM Verzeichniskonten vorhanden. Die Eigentümer werden in den Standard-Entscheidungsworkflows als Entscheider und Attestierer berücksichtigt.

  Weitere Informationen finden Sie unter Eigentümer von PAM Objekten auf Seite 167.

Zielsystemverantwortliche für PAM Systeme

Im One Identity Manager ist eine Standardanwendungsrolle für die Zielsystemverantwortlichen vorhanden. Weisen Sie dieser Anwendungsrolle die Personen zu, die berechtigt sind, alle Appliances im One Identity Manager zu bearbeiten.

Wenn Sie die Berechtigungen der Zielsystemverantwortlichen auf einzelne Appliances einschränken wollen, definieren Sie weitere Anwendungsrollen. Die Anwendungsrollen müssen der Standardanwendungsrolle untergeordnet sein.

Ausführliche Informationen zum Einsatz und zur Bearbeitung von Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

1. Der One Identity Manager Administrator legt Personen als Zielsystemadministratoren fest.
2. Die Zielsystemadministratoren nehmen die Personen in die Standardanwendungsrolle für die Zielsystemverantwortlichen auf.

   Zielsystemverantwortliche der Standardanwendungsrolle sind berechtigt alle Privileged Account Management Systeme im One Identity Manager zu bearbeiten.
3. Zielsystemverantwortliche können innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche berechtigen und bei Bedarf weitere untergeordnete Anwendungsrollen erstellen und einzelnen PAM Systemen zuweisen.

Tabelle 31: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Privileged Account Management** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen. • Berechtigen innerhalb ihres Verantwortungsbereiches Personen als Eigentümer von privilegierten Objekten.

Um initial Personen als Zielsystemadministrator festzulegen

1. Melden Sie sich als One Identity Manager Administrator (Anwendungsrolle **Basisrollen | Administratoren**) am Manager an.
2. Wählen Sie die Kategorie **One Identity Manager Administration > Zielsysteme > Administratoren**.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Person zu und speichern Sie die Änderung.

Um initial Personen in die Standardanwendungsrolle für Zielsystemverantwortliche aufzunehmen

1. Melden Sie sich als Zielsystemadministrator (Anwendungsrolle **Zielsysteme | Administratoren**) am Manager an.
2. Wählen Sie die Kategorie **One Identity Manager Administration > Zielsysteme > Privileged Account Management**.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Personen zu und speichern Sie die Änderungen.

Um als Zielsystemverantwortlicher weitere Personen als Zielsystemverantwortliche zu berechtigen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie in der Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Zielsystemverantwortliche** die Anwendungsrolle.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Personen zu und speichern Sie die Änderungen.

Um Zielsystemverantwortliche für einzelne Privileged Account Management Systeme festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **Privileged Account Management > Appliances**.
3. Wählen Sie in der Ergebnisliste die Appliance.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Zielsystemverantwortliche** die Anwendungsrolle.

   - ODER -

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

   a. Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Zielsysteme | Privileged Account Management** zu.

   b. Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.

6. Speichern Sie die Änderungen.
7. Weisen Sie der Anwendungsrolle die Personen zu, die berechtigt sind, das System im One Identity Manager zu bearbeiten.

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung eines Privileged Account Management Systems auf Seite 11
- Allgemeine Stammdaten von PAM Appliances auf Seite 129

Jobserver für PAM-spezifische Prozessverarbeitung

Für die Verarbeitung der zielsystemspezifischen Prozesse im One Identity Manager muss der Synchronisationsserver mit seinen Serverfunktionen bekannt sein. Um die Funktion eines Servers zu definieren, haben Sie mehrere Möglichkeiten:

- Erstellen Sie im Designer in der Kategorie **Basisdaten > Installationen > Jobserver** einen Eintrag für den Jobserver. Ausführliche Informationen dazu finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Wählen Sie im Manager in der Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Server** einen Eintrag für den Jobserver aus und bearbeiten Sie die Stammdaten des Jobservers.

  Nutzen Sie dieses Verfahren, wenn der Jobserver bereits im One Identity Manager bekannt ist und Sie für den Jobserver spezielle Funktionen konfigurieren möchten.

Verwandte Themen

- Systemanforderungen für den One Identity Safeguard Synchronisationsserver auf Seite 19
- PAM Jobserver bearbeiten auf Seite 178

PAM Jobserver bearbeiten

Um einen Jobserver und seine Funktionen zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Privileged Account Management > Basisdaten zur Konfiguration > Server**.
2. Wählen Sie in der Ergebnisliste den Jobserver-Eintrag.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

4. Bearbeiten Sie die Stammdaten für den Jobserver.
5. Wählen Sie die Aufgabe **Serverfunktionen zuweisen** und legen Sie die Serverfunktionen fest.
6. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Jobserver auf Seite 179
- Festlegen der Serverfunktionen auf Seite 182
- One Identity Manager Service mit One Identity Safeguard Konnektor installieren auf Seite 20

Allgemeine Stammdaten für Jobserver

HINWEIS: Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten > Installationen > Jobserver** zur Verfügung.

HINWEIS: Abhängig von den installierten Modulen können weitere Eigenschaften verfügbar sein.

Tabelle 32: Eigenschaften eines Jobservers

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS Syntax. Syntax: `<Name des Servers>.<Vollqualifizierter Domänenname>`
Zielsystem	Zielsystem des Computerkontos.
Sprachkultur	Sprache des Servers.
Server ist Cluster	Gibt an, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. HINWEIS: Die Eigenschaften **Server ist Cluster** und **Server gehört zu Cluster** schließen einander aus.
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.
IP-Adresse (IPv4)	Internet Protokoll Version 4 (IPv4)-Adresse des Servers.
Kopierverfahren (Quellserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Quelle einer Kopieraktion ist. Derzeit werden nur Kopierverfahren über die Programme `Robocopy` und `rsync` unterstützt.

Eigenschaft	Bedeutung
	Wird kein Verfahren angegeben, ermittelt der One Identity Manager Service zur Laufzeit das Betriebssystem des Servers, auf dem die Kopieraktion ausgeführt wird. Die Replikation erfolgt dann zwischen Servern mit einem Windows Betriebssystem mit dem Programm `Robocopy` und zwischen Servern mit einem Linux Betriebssystem mit dem Programm `rsync`. Unterscheiden sich die Betriebssysteme des Quellservers und des Zielservers, so ist für eine erfolgreiche Replikation die Angabe der zulässigen Kopierverfahren zwingend erforderlich. Es wird das Kopierverfahren eingesetzt, das beide Server unterstützen.
Kopierverfahren (Zielserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Ziel einer Kopieraktion ist.
Codierung	Codierung des Zeichensatzes mit der Dateien auf dem Server geschrieben werden.
Übergeordneter Jobserver	Bezeichnung des übergeordneten Jobservers.
Ausführender Server	Bezeichnung des ausführenden Servers. Eingetragen wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden. Diese Angabe wird bei der automatischen Aktualisierung des One Identity Manager Service ausgewertet. Verarbeitet ein Server mehrere Queues, wird mit der Auslieferung von Prozessschritten solange gewartet, bis alle Queues, die auf demselben Server abgearbeitet werden, die automatische Aktualisierung abgeschlossen haben.
Queue	Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Mit dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Serverbetriebssystem	Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte **Win32**, **Windows**, **Linux** und **Unix**. Ist die Angabe leer, wird **Win32** angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server

Eigenschaft	Bedeutung
	entsprechend einzutragen.
One Identity Manager Service installiert	Gibt an, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur `QBM_PJobQueueLoad` aktiviert, sobald die Queue das erste Mal angefragt wird. Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.
Stopp One Identity Manager Service	Gibt an, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten. Den Dienst können Sie mit entsprechenden administrativen Berechtigungen im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*.
Pausiert wegen Nicht-verfügbarkeit eines Zielsystems	Gibt an, ob die Verarbeitung von Aufträgen für diese Queue angehalten wurde, weil das Zielsystem, für den dieser Jobserver der Synchronisationsserver ist, vorübergehend nicht erreichbar ist. Sobald das Zielsystem wieder erreichbar ist, wird die Verarbeitung gestartet und alle anstehenden Aufträge werden ausgeführt. Ausführliche Informationen zum Offline-Modus finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.
Kein automatisches Softwareupdate	Gibt an, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.
Softwareupdate läuft	Gibt an, ob gerade eine Softwareaktualisierung ausgeführt wird.
Serverfunktion	Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

Verwandte Themen

- Festlegen der Serverfunktionen auf Seite 182

Festlegen der Serverfunktionen

HINWEIS: Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten > Installationen > Jobserver** zur Verfügung.

Die Serverfunktion definiert die Funktion eines Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

HINWEIS: Abhängig von den installierten Modulen können weitere Serverfunktionen verfügbar sein.

Tabelle 33: Zulässige Serverfunktionen

Serverfunktion	Anmerkungen
Aktualisierungsserver	Der Server führt die automatische Softwareaktualisierung aller anderen Server aus. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Der Server kann SQL Aufträge ausführen. Bei der initialen Schemainstallation wird der Server, auf dem die One Identity Manager-Datenbank installiert ist, mit dieser Serverfunktion gekennzeichnet.
SQL Ausführungsserver	Der Server kann SQL Aufträge ausführen. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Für eine Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.
CSV Skriptserver	Der Server kann CSV-Dateien per Prozesskomponente `ScriptComponent` verarbeiten.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
SMTP Host	Server, auf dem durch den One Identity Manager Service E-Mail Benachrichtigungen verschickt werden. Voraussetzung zum Versenden von Mails durch den One Identity Manager Service ist ein konfigurierter SMTP Host.
Standard Berichtsserver	Server, auf dem die Berichte generiert werden.
One Identity Safeguard Konnektor	Server, auf dem der One Identity Safeguard Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem One Identity Safeguard aus.

Verwandte Themen

- Allgemeine Stammdaten für Jobserver auf Seite 179

Anhang A

Konfigurationsparameter für die Verwaltung eines Privileged Account Management Systems

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

Tabelle 34: Konfigurationsparameter für die Synchronisation eines Privileged Account Management Systems

Konfigurationsparameter	Bedeutung bei Aktivierung
TargetSystem | PAG	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung von Privileged Account Management Systemen. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der 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*.
TargetSystem | PAG | Accounts	Erlaubt die Konfiguration der Angaben zu PAM Benutzerkonten.
TargetSystem | PAG | Accounts | InitialRandomPassword	Gibt an, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in der zugewiesenen Kennwortrichtlinie definiert sind.
TargetSystem | PAG | Accounts |	Person, die E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der

Konfigurationsparameter	Bedeutung bei Aktivierung
InitialRandomPassword | SendTo	Kostenstelle/Abteilung/Standort/Geschäftsrolle, Verantwortlicher der Person oder `XUserInserted`). Ist kein Empfänger ermittelbar, dann wird die E-Mail an die im Konfigurationsparameter **TargetSystem | PAG | DefaultAddress** hinterlegte Adresse versandt.
TargetSystem | PAG | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Anmeldeinformationen zum Benutzerkonto zu versorgen. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto** verwendet.
TargetSystem | PAG | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Informationen zum initialen Kennwort zu versorgen. Es wird die Mailvorlage **Person - Initiales Kennwort für neues Benutzerkonto** verwendet.
TargetSystem | PAG | Accounts | MailTemplateDefaultValues	Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto mit Standardwerten** verwendet.
TargetSystem | PAG | Accounts | PrivilegedAccount	Erlaubt die Konfiguration der Einstellungen für privilegierte Benutzerkonten.
TargetSystem | PAG | Accounts | TransferJPegPhoto	Gibt an, ob bei Änderung des Bildes in den Stammdaten der Person dieses an bestehende Benutzerkonten publiziert wird. Das Bild ist nicht Bestandteil der normalen Synchronisation, es wird nur bei Änderung der Personenstammdaten publiziert.
TargetSystem | PAG | DefaultAddress	Standard-E-Mail-Adresse des Empfängers von Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem | PAG | PersonAutoDefault	Modus für die automatische Personenzuordnung für Benutzerkonten, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem | PAG | PersonAutoDisabledAccounts	Gibt an, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem | PAG | PersonAutoFullsync	Modus für die automatische Personenzuordnung für Benutzerkonten, die durch die Synchronisation in der

Konfigurationsparameter	Bedeutung bei Aktivierung
	Datenbank angelegt oder aktualisiert werden.
TargetSystem | PAG | PersonExcludeList	Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird. Beispiel: `ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $`
TargetSystem | PAG | UserObjectAccessThreshold	Grenzwert für die Anzahl privilegierter Zugriffsberechtigungen pro Benutzer, bei dessen Überschreiten der Risikoindex des Benutzers erhöht wird. Standard ist **20**.
TargetSystem | PAG | HighRiskIndexThreshold	Risikoindexwerte, die höher als dieser Grenzwert sind, werden als **hoch** bewertet. Standard ist **0,5**.
QER | ITShop | AutoPublish | PAGUsrGroup	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der automatischen Übernahme von PAM Benutzergruppen in den IT Shop. Ist der Parameter aktiviert, werden alle Benutzergruppen automatisch als Produkte dem IT Shop zugewiesen. Die Änderung des Parameters erfordert eine Kompilierung der 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*.
QER | ITShop | AutoPublish | PAGUsrGroup | ExcludeList	Auflistung aller PAM Benutzergruppen, für die keine automatische Zuordnung zum IT Shop erfolgen soll. Jeder Eintrag ist Bestandteil eines regulären Suchmusters und unterstützt die Notation für reguläre Ausdrücke. Beispiel: `.*Administrator.*|.*Admins|.*Operators`

Anhang B

Standardprojektvorlage für One Identity Safeguard

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.

Die Projektvorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 35: Abbildung der One Identity Safeguard Schematypen auf Tabellen im One Identity Manager Schema

Schematyp in der One Identity Safeguard	Tabelle im One Identity Manager Schema
Appliance	PAGAppliance
IdentityProvider	PAGIdentityProvider
AuthenticationProvider	PAGAuthProvider
User	PAGUser
UserGroup	PAGUsrGroup
Entitlement	PAGEntl
AccessRequestPolicy	PAGReqPolicy
AcountGroup	PAGAccGroup
Asset	PAGAsset
AssetAccount	PAGAstAccount
AssetGroup	PAGAstGroup

Schematyp in der One Identity Safeguard	Tabelle im One Identity Manager Schema
Directory	PAGDirectory
DirectoryAccount	PAGDirAccount

Anhang C

Verarbeitung von One Identity Safeguard Systemobjekten

Folgende Tabelle beschreibt die zulässigen Verarbeitungsmethoden für die One Identity Safeguard Schematypen und benennt notwendige Einschränkungen bei der Verarbeitung der Systemobjekte.

Tabelle 36: Zulässige Verarbeitungsmethoden für Schematypen

Schematyp	Lesen	Einfügen	Löschen	Aktualisieren
Appliance (`Appliance`)	ja	nein	nein	nein
Benutzerkonto (`User`)	ja	ja	ja	ja
Benutzergruppe (`UserGroup`)	ja	nein	nein	ja
Identitätsanbieter (`IdentityProvider`)	ja	nein	nein	nein
Authentifizierungsanbieter (`AuthenticationProvider`)	ja	nein	nein	nein
Verzeichnis (`Directory`)	ja	nein	nein	nein
Verzeichniskonto (`DirectoryAccount`)	ja	nein	nein	nein
Asset (`Asset`)	ja	nein	nein	nein
Konto (`AssetAccount`)	ja	nein	nein	nein
Assetgruppe(`AssetGroup`)	ja	nein	nein	nein
Kontogruppe (`AccountGroup`)	ja	nein	nein	nein
Nutzungsrecht (`Entitlement`)	ja	nein	nein	nein
Zugriffsanforderungsrichtlinie (`AccessRequestPolicy`)	ja	nein	nein	nein

Anhang D

Einstellungen des One Identity Safeguard Konnektors

Für die Systemverbindung mit dem One Identity Safeguard Konnektor werden die folgenden Einstellungen konfiguriert.

Tabelle 37: Einstellungen des One Identity Safeguard Konnektors

Einstellung	Beschreibung
Anzeigename der Appliance	Anzeigename der Appliance. Variable: `CP_ApplianceDisplay`
Systembezeichner	Eindeutiger Bezeichner zur Identifizierung der Appliance. Variable: `CP_ApplianceID` **VORSICHT: Der Systembezeichner muss die Appliance eindeutig beschreiben. Anhand der Systembezeichners werden die Appliances unterschieden. Die mehrfache Vergabe eines Bezeichners für unterschiedliche Appliances kann zu Fehlverhalten und Datenverlust führen.**
Immer zu primärer Appliance im Cluster verbinden	Diese Option wird automatisch gesetzt, wenn beim Testen der Verbindungsdaten ein One Identity Safeguard Cluster erkannt wird. Wenn Sie einen Cluster aus mehreren One Identity Safeguard Appliances verwenden, sollte diese Option aktiviert sein. Variable: `CP_ConnectPrimaryNode`
Appliance Hostname oder IP	Hostname oder IP- Adresse der Appliance. Wenn Sie einen Cluster aus mehreren One Identity Safeguard Appliances verwenden, ist hier die primäre Appliance einzutragen. Variable: `CP_ApplianceHost`
Fingerabdruck des vertrauenswürdigen	Fingerabdruck des vertrauenswürdigen Zertifikates, welches vom Synchronisationsbenutzer und vom Benutzerkonto des One

Einstellung	Beschreibung
Zertifikates	Identity Manager Service genutzt wird. Variable: `CP_CertificateThumbprint`
Ignoriere SSL Verbindungsfehler	Diese Option sollten Sie nur zu Testzwecken aktivieren, da hier potentiell Verbindungen vertraut wird, die nicht sicher sind. Variable: `CP_IgnoreSSLErrors` Standard: **False**
Cluster IPv4 Addresses	Semikolongetrennte Liste von IPv4 Adressen einer Umgebung aus mehreren Appliances (Cluster). Variable: `CP_ClusterIPv4Addresses`
Cluster IPv6 Addresses	Semikolongetrennte Liste von IPv6 Adressen einer Umgebung aus mehreren Appliances (Cluster). Variable: `CP_ClusterIPv6Addresses`
Konnektordefinition anpassen	Mit dieser Einstellung können Sie die Definition anpassen, die vom Konnektor verwendet wird. WICHTIG: Die Konnektordefinition sollte nur mit Anweisungen eines Support-Mitarbeiters geändert werden. Änderungen an dieser Einstellung haben weitreichende Auswirkungen in der Synchronisation und müssen deshalb sehr vorsichtig behandelt werden. HINWEIS: Eine angepasste Konnektordefinition wird nicht standardmäßig überschrieben, wenn eine neue Version des Konnektors beziehungsweise eine aktualisierte Konnektordefinition herausgegeben wird.

Anhang E

Bekannte Probleme bei der Anbindung einer One Identity Safeguard Appliance

Problem

Bei der Einrichtung eines Synchronisationsprojektes für One Identity Safeguard wird eine Fehlermeldung angezeigt:

```
404: Not Found -- 0:
```

Ursache

Es wird eine ältere One Identity Safeguard Version verwendet, die nicht von One Identity Manager unterstützt wird.

Lösung

Stellen Sie sicher, dass mindestens die One Identity Safeguard Version 6.0 verwendet wird. Weitere Informationen finden Sie unter Synchronisieren eines Privileged Account Management Systems auf Seite 15.

Problem

Bei Bestellung eines Zugriffs auf ein Asset aus dem Bereich einer Zugriffsanforderungsrichtlinie, die für assetbasierten Sitzungszugriff vom Typ **Benutzer angegeben** konfiguriert ist, tritt im One Identity Safeguard folgender Fehler auf:

```
400: Bad Request -- 60639: A valid account must be identified in the request.
```

Die Bestellung wird im One Identity Manager abgelehnt und der Fehler in der Bestellung als Begründung angezeigt.

Lösung

Das Problem wurde mit One Identity Safeguard Version 2.6 behoben.

Problem

Die Verbindung des One Identity Safeguard Konnektors zur One Identity Safeguard Appliance wird mit folgenden Fehlermeldungen abgebrochen:

```
The version <Appliance version> of the connected One Identity Safeguard appliance is not supported by this version of the One Identity Manager Safeguard connector. Error-free operation cannot be guaranteed. The connection is terminated.
```

```
The version <safeguard-ps version> of the PowerShell module 'safeguard-ps' does not match the version <Appliance version> of the One Identity Safeguard appliance. The connection is terminated
```

Ursache

Die Version der einsetzten One Identity Safeguard Appliance passt nicht zur Version des verwendeten Windows PowerShell Moduls **safeguard-ps**.

Lösung

Stellen Sie sicher, dass Sie die passenden Versionen verwenden. Die Major-Version und die Minor-Version des Windows PowerShell Moduls müssen mit der Major-Version und der Minor-Version Ihrer One Identity Safeguard Appliance übereinstimmen müssen.

Weitere Informationen finden Sie unter Windows PowerShell Modul safeguard-ps installieren auf Seite 20.

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

Anmeldeinformationen 125

Anwendungsrolle

- Asset und Konteneigentümer 11, 167
- Privileged Account Governance 11, 167

Anwendungsrollen für die Privileged Account Management 11

Ausschlussdefinition 105

Ausstehendes Objekt 49

B

Basisobjekt 36, 42

Benutzerkonto

- administratives Benutzerkonto 88-90
- Automatisierungsgrad 84
- Bildungsregeln ausführen 68
- Gruppenidentität 90
- Identität 86
- Kategorie 108
- persönliche Administratoridentität 89
- privilegiertes Benutzerkonto 86, 91
- Standardbenutzerkonto 87
- Typ 86-87, 89-91
- verbunden 84

Bildungsregel

- IT Betriebsdaten ändern 68

E

E-Mail-Benachrichtigung 125

Einzelobjekt synchronisieren 47

Einzelobjektsynchronisation 42, 47

- beschleunigen 43

I

Identität

- Dienstidentität 86
- Gruppenidentität 86, 90
- Organisatorische Identität 86
- Persönliche Administratoridentität 86, 89
- Primäre Identität 86
- Zusatzidentität 86

IT Betriebsdaten

- ändern 68
- erfassen 67

IT Shop Regal

- Kontendefinitionen zuweisen 73

J

Jobserver 178

- bearbeiten 20, 178
- Eigenschaften 179
- Lastverteilung 43

K

Kategorie 131

Kennwort

- initial 124-125

Kennwortrichtlinie 112

- Anzeigename 117

Ausschlussliste 123
bearbeiten 116
Fehlanmeldungen 117
Fehlermeldung 117
Generierungsskript 120, 122
initiales Kennwort 117
Kennwort generieren 124
Kennwort prüfen 123
Kennwortalter 117
Kennwortlänge 117
Kennwortstärke 117
Kennwortzyklus 117
Namensbestandteile 117
Prüfskript 120
Standardrichtlinie 114, 117
Vordefinierte 113
Zeichenklassen 119
zuweisen 114
Konfigurationsparameter 14, 184
Kontendefinition 57
an Abteilung zuweisen 71
an alle Personen zuweisen 72
an Appliance zuweisen 75
an Benutzerkonten zuweisen 84
an Geschäftsrolle zuweisen 71
an Kostenstelle zuweisen 71
an Person zuweisen 69, 72
an Standort zuweisen 71
an Systemrollen zuweisen 73
automatisch zuweisen 72
Automatisierungsgrad 62-63
bearbeiten 59
erstellen 58
in IT Shop aufnehmen 73
IT Betriebsdaten 65, 67
löschen 76

L

Lastverteilung 43

M

Mitgliedschaft
Änderung provisionieren 40

N

NLog 52

O

Objekt
ausstehend 49
publizieren 49
sofort löschen 49
Offline-Modus 53

P

PAM Appliance
Berichte 160
erstellen 128
Kategorie 108, 129
Kategorien festlegen 131
Kontendefinition (initial) 75, 129
Personenzuordnung 81
Überblick 132
Zielsystemverantwortliche 129, 175
PAM Asset 154
Eigentümer 168, 170
PAM Assetgruppe 155
Eigentümer 168, 170

PAM Assetkonto 155
Eigentümer 168, 170
Risikoindex 155
PAM Authentifizierungsanbieter
Certificate 134
Local 134
Verzeichnis 135
PAM Benutzergruppe 149
an Abteilung zuweisen 97
an Geschäftsrollen zuweisen 98
an Kostenstelle zuweisen 97
an Standort zuweisen 97
ausschließen 105
bearbeiten 150
Benutzerkonto zuweisen 94, 104
in IT Shop aufnehmen 100
in IT Shop aufnehmen (automatisch) 102
in Systemrolle aufnehmen 99
Kategorie 108
Kategorie zuordnen 150
Leistungsposition 102
Produkteigner 102
Regal 102
Risikoindex 150
über IT Shop bestellen 150
Überblick 154
Übersicht aller Zuweisungen 110
Vererbung über Kategorien 131
Vererbung über Rollen 94
wirksam 105
Zusatzeigenschaft zuweisen 153
PAM Benutzerkonto 132
bearbeiten 137
Benutzergruppe zuweisen 104
Datenqualität 160
erstellen 134-135
Kennwort 124
Benachrichtigung 125
lokal 134
löschen 148
Löschverzögerung 92, 148
PAM Appliance 138
Person zuordnen 79
Risikoindex 138
sperren 147-148
Überblick 149
Verzeichnisbenutzer 135
wiederherstellen 148
zertifikatsbasiert 134
zugeordnete Person 138
Zusatzeigenschaft zuweisen 146
PAM Eigentümer 167-168, 170
PAM Kontogruppe 157
Eigentümer 168, 170
PAM Nutzungsrecht 159
PAM Verzeichnis 158
PAM Verzeichniskonto 156
Eigentümer 168, 170
PAM Zugriffsanforderung 164
bestellen 166
Entscheidungsrichtlinie 166
Entscheidungsworkflow 166
Kennwortanforderung 166
Regal 166
Remote-Desktop-Sitzungs-anforderung 166
Servicekategorie 166
SSH-Schlüssel-Anforderung 166
SSH-Sitzungsanforderung 166

Systemanforderungen 165
Telnet-Sitzungsanforderung 166
PAM Zugriffsanforderungsrichtlinie 160
konfigurieren 171
Person
PAM Benutzerkonto zuweisen 85
Personenzuordnung
entfernen 82
manuell 82
Suchkriterium 81
Privileged Account Management
Eigentümer 11
Zielsystemverantwortlicher 11
Projektvorlage 187
Protokolldatei 52
Provisionierung
beschleunigen 43
Mitgliederliste 40

R

Revision zurücksetzen 52
Revisionsfilter 40
Risikobewertung
PAM Benutzergruppe 150
PAM Benutzerkonto 138

S

Schema
aktualisieren 39
Änderungen 39
komprimieren 39
Server 178
Serverfunktion 182
Standardbenutzerkonto 87
Startinformation zurücksetzen 52
Startkonfiguration 36
Synchronisation
Basisobjekt
erstellen 35
Benutzer 17
Berechtigungen 17
beschleunigen 40
Erweitertes Schema 35
konfigurieren 28, 33
Scope 33
simulieren 52
starten 28, 45
Synchronisationsprojekt
erstellen 28
Variable 33
Variablenset 35
Verbindungsparameter 28, 33, 35
verhindern 47
verschiedene Appliances 35
Voraussetzung 15
Workflow 28, 34
Zeitplan 45
Zielsystemschema 35
Synchronisationsanalysebericht 52
Synchronisationskonfiguration
anpassen 33-35
Synchronisationsprojekt
bearbeiten 132
deaktivieren 47
erstellen 28
Projektvorlage 187
Synchronisationsprotokoll 46, 52
erstellen 32
Inhalt 32

Synchronisationsrichtung
In das Zielsystem 28, 34
In den Manager 28
Synchronisationsserver 19, 178
bearbeiten 178
installieren 20
Jobserver 20
konfigurieren 19-20
Serverfunktion 182
Systemanforderungen 19-20
Synchronisationsworkflow
erstellen 28, 34
Systemverbindung
aktives Variablenset 37
ändern 35

V

Variablenset 36
aktiv 37
Verbindungsparameter umwandeln 36
Vererbung
Kategorie 108

Z

Zeitplan 45
deaktivieren 47
Zielsystem
nicht verfügbar 53
Zielsystemabgleich 49
Zusatzeigenschaft
PAM Benutzergruppe 153
PAM Benutzerkonto 146