One Identity Manager 8.1.4

Administrationshandbuch für die Anbindung einer IBM Notes Umgebung

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 die Anbindung einer IBM Notes Umgebung
Aktualisiert - 19. Oktober 2020, 08:23 Uhr
Version - 8.1.4

Inhalt

1

Verwalten einer IBM Notes-Umgebung

Mit dem One Identity Manager werden die Objekte einer IBM Notes-Umgebung wie Benutzer, Gruppen, Mail-In-Datenbanken, Server, Richtlinien und Zertifikate verwaltet. Durch die Definition von Notes Domänen im One Identity Manager ist die Administration mehrerer produktiver IBM Notes-Umgebungen parallel mit einer One Identity Manager-Datenbank möglich. Notes Benutzer und Personendokumente werden im One Identity Manager als Benutzerkonten verwaltet.

Im One Identity Manager werden die Personen eines Unternehmens mit den benötigten Benutzerkonten versorgt. Dabei können unterschiedliche Mechanismen für die Verbindung der Personen mit ihren Notes Benutzerkonten genutzt werden. Ebenso können die Benutzerkonten getrennt von Personen verwaltet und somit administrative Benutzerkonten eingerichtet werden.

Bei der Zertifizierung neuer Benutzer müssen eine Reihe benutzerspezifischer Dateien generiert werden, die dem Benutzer für die Arbeit mit IBM Notes zur Verfügung stehen müssen. Beim Anlegen eines Benutzers durch den IBM Notes Konnektor werden die Benutzer-ID-Datei zur Authentifizierung, die Postfachdatei sowie das persönliche Adressbuch des Benutzers erzeugt.

Neben Benutzerkonten werden Gruppen und Mail-In-Datenbanken über den One Identity Manager verwaltet. Gruppen werden eingesetzt, um den Benutzern die benötigten Zugriffsberechtigungen zur Verfügung zu stellen oder werden als Mailverteilerliste genutzt. Über gemeinsam genutzte Mail-In-Datenbanken können die Benutzer Nachrichten versenden oder empfangen. Über die Vergabe von Rechten können die Benutzer auf diese Mail-In-Datenbanken zugreifen. Beim Anlegen einer Mail-In-Datenbank über den One Identity Manager wird die benötigte Postfachdatei erzeugt.

Serverdokumente, Zertifikate, Richtlinien und Schablonen für Postfachdateien werden lediglich in die One Identity Manager-Datenbank eingelesen, damit sie beim Einrichten von Benutzerkonten und Gruppen referenziert werden können. Für Serverdokumente können im One Identity Manager Zugriffslisten definiert werden, um festzulegen, wer für verschiedene Zwecke Zugriff auf einen Server hat.

Architekturüberblick

Im One Identity Manager wird der Sichtbarkeitsbereich einer produktiven IBM Notes-Umgebung als Notes Domäne abgebildet. Für die Synchronisation benötigt der One Identity Manager Zugriff auf das Domino-Verzeichnis dieser IBM Notes-Umgebung.

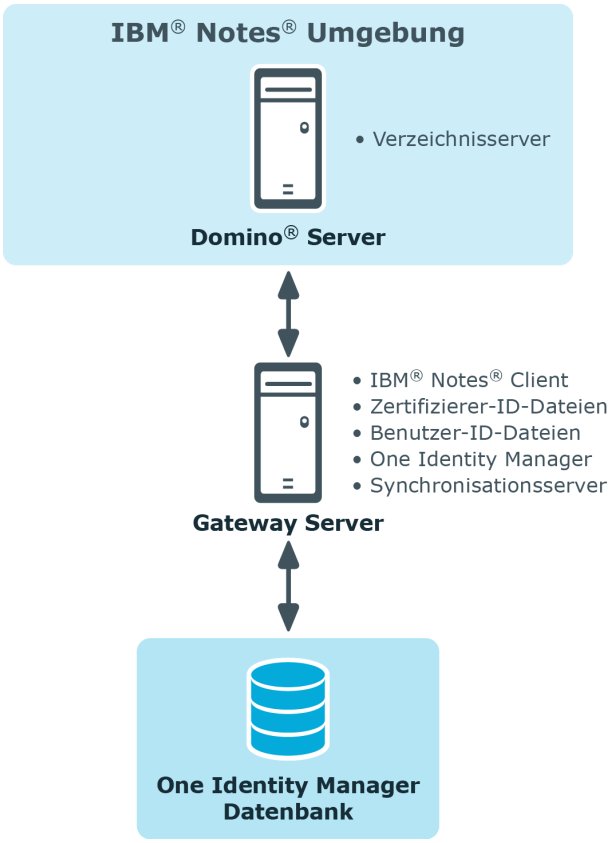
Innerhalb der One Identity Manager-Umgebung wird ein Server definiert, der alle administrativen Aufgaben, die IBM Notes-Umgebung betreffend, ausführt. Dieser Server wird im Folgenden als Gateway Server bezeichnet. Der Gateway Server übernimmt die Funktion des Synchronisationsservers. Er ist selbst kein produktiver Domino-Server. Auf dem Gateway Server werden ein IBM Notes Client, der One Identity Manager Service und der IBM Notes Konnektor installiert.

Vom Gateway Server werden alle Aktionen des IBM Notes Konnektors ausgeführt. Bei der Ausführung der Aktionen im Zielsystem kommuniziert der Gateway Server mit einem Domino-Server der produktiven Umgebung. Dieser Domino-Server ist ein ausgewählter Server mit guter Netzwerkanbindung zum Gateway Server. Da der IBM Notes Konnektor Zugriff auf das Domino-Verzeichnis benötigt, nutzen Sie dafür vorzugsweise einen Verzeichnisserver.

Für die Synchronisation stellen Sie eine ID-Datei zum Zugriff auf die produktive IBM Notes-Umgebung mit ausreichenden administrativen Rechten zur Verfügung. Sofern nicht mit einem Certification-Authority-Prozess (CA-Prozess) gearbeitet werden soll, muss eine Zertifizierer-ID-Datei bereitgestellt werden. Beide Dateien müssen auf dem Gateway Server verfügbar sein.

Der Gateway Server führt über den One Identity Manager Service Aktionen wie Zertifizierungen, Anlegen, Ändern und Löschen von Dokumenten im Domino-Verzeichnis aus. Außerdem können über diesen Weg Datenbanken für Benutzer, Postfachdateien oder Mail-In-Datenbanken auf den Domino-Servern angelegt werden. Der One Identity Manager Service stellt einen IBM Notes-Client-Kontext unter Verwendung der IBM Domino COM-Library her und verarbeitet darin alle notwendigen Funktionen zum Datenaustausch mit dem Domino-Server (Zugriff auf Domino-Objekte, Ausführen von Notes-Agenten, Erzeugen von administrativen Prozessen (AdminP), Fehlerbehandlung).

Abbildung 1: Kommunikation des IBM Notes Konnektors mit der IBM Notes-Umgebung



Die Objekte einer IBM Notes-Umgebung werden in der One Identity Manager-Datenbank folgendermaßen abgebildet:

Tabelle 1: Abbildung von Objekttypen einer IBM Notes-Umgebung im One Identity Manager

IBM Domino	One Identity Manager
Domino-Server	Notes Server
Domino-Domäne	Keine direkte Abbildung.
	Notes Domäne Eigenschaft von Notes Objekten, um die Objekte verschiedenen IBM Notes-Umgebungen zuzuordnen.
Benutzer	Notes Benutzerkonto
Gruppe	Notes Gruppe

IBM Domino	One Identity Manager
Mail-In-Datenbank	Notes Mail-In-Datenbank
Notes Zertifikat	Notes Zertifikat
Schablone	Notes Schablone
Richtlinie	Notes Richtlinie

One Identity Manager Benutzer für die Verwaltung einer IBM Notes-Umgebung

In die Einrichtung und Verwaltung einer IBM Notes-Umgebung sind folgende Benutzer eingebunden.

Tabelle 2: 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 | IBM Notes** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle:

Benutzer	Aufgaben
	• Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen. • 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.
One Identity Manager Administratoren	• Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.
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**

Benutzer	Aufgaben
	zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an Abteilungen, Kostenstellen und Standorte zu.
Administratoren für Geschäftsrollen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Geschäftsrollen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an Geschäftsrollen zu.

Einrichten der Synchronisation mit einer IBM Notes-Umgebung

Der One Identity Manager unterstützt die Synchronisation mit IBM Notes-Umgebungen in den folgenden Versionen:

- IBM Domino Server Version 8, 9 und 10
- HCL Domino Server Version 11
- IBM Notes Client Version 8.5.3 oder 10.0
- HCL Notes Client Version 11.0.1

Um die Objekte einer IBM Notes-Umgebung initial in die One Identity Manager-Datenbank einzulesen

1. Stellen Sie in der IBM Notes-Umgebung einen Benutzer für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Die One Identity Manager Bestandteile für die Verwaltung von IBM Notes-Umgebungen sind verfügbar, wenn der Konfigurationsparameter "TargetSystem\NDO" aktiviert ist.
    - Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.
    - 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 den Gateway Server.
4. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.
5. Wenn durch den IBM Notes Konnektor Benutzerkonten in der IBM Notes-Umgebung registriert werden sollen, passen Sie die dafür benötigten Zertifikate im One Identity Manager an. Geben Sie den Pfad zur ID-Datei des Zertifizierers oder den Namen der CA-Datenbank an.

Detaillierte Informationen zum Thema

- Benutzer und Berechtigungen für die Synchronisation mit einer IBM Notes-Umgebung auf Seite 16
- Installation und Konfiguration eines Gateway Servers auf Seite 18
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Notes Domäne auf Seite 25
- Allgemeine Stammdaten für Notes Zertifikate auf Seite 92

Benutzer und Berechtigungen für die Synchronisation mit einer IBM Notes-Umgebung

Bei der Synchronisation des One Identity Manager mit einer IBM Notes-Umgebung spielen folgende Benutzer eine Rolle.

Tabelle 3: Benutzer für die Synchronisation

Benutzer	Berechtigungen
Benutzerkonto des One Identity Manager Service	Das Benutzerkonto für den One Identity Manager Service benötigt die Rechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Rechte vergeben, 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 Rechte 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 Rechte 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.

Benutzer	Berechtigungen
	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)
Benutzer für den Zugriff auf das Zielsystem (Synchronisationsbenutzer)	Der Benutzer für den Zugriff auf das Zielsystem benötigt ausreichend administrative Rechte auf das Domino-Verzeichnis (`names.nsf`). Die Mindestanforderungen sind: • Zugriffsfunktion „Editor" auf das primäre Domino-Verzeichnis • Rechte zum Löschen von Dokumenten • Zusätzlich zu den Standardrechten die Rolle „UserCreator" • Remotekonsolenberechtigungen • Administrativer Zugriff auf einen Domino-Server (Server, auf dem die Registrierung neuer Benutzerkonten sowie das Erstellen von AdminP-Aufträgen möglich ist) Die Zugriffsfunktion „Editor" wird zusätzlich für folgende Datenbanken benötigt: • certlog.nsf • admin4.nsf
Benutzer für den Zugriff auf die One Identity Manager-Datenbank	Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer **Synchronization** bereitgestellt.

Konfiguration des Domino-Servers

Nehmen Sie auf dem Domino-Server, mit dem der Gateway Server kommuniziert, folgende Einstellungen vor:

- Richten Sie für das Domino-Verzeichnis einen Volltextindex ein.
- Setzen Sie in der Datei `Notes.ini` `FT_MAX_SEARCH_RESULTS=2147483000`.

  Bei der Anwendung von Filtern im Domino-Verzeichnis werden standardmäßig maximal 5000 gefilterte Werte zurückgegeben. Um eine vollständige Ergebnisliste der Elemente, die der Filterbedingung genügen, zu erhalten, muss dieser Wert in der

Datei `Notes.ini` des Domino-Servers mit dem hier benannten Wert überschrieben werden.

Ausführliche Informationen entnehmen Sie der Dokumentation Ihrer IBM Notes-Umgebung.

Installation und Konfiguration eines Gateway Servers

Die Funktion des Synchronisationsservers wird durch den Gateway Server wahrgenommen. Zur Einrichtung eines Gateway Servers muss ein Computer bereitgestellt werden, auf dem die nachfolgend genannte Software installiert ist:

- Windows Betriebssystem

  Unterstützt werden die Versionen:

  - Windows Server 2008 R2 (nicht-Itanium 64-Bit) ab Service Pack 1
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
- Microsoft .NET Framework Version 4.7.2 oder höher

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.
- Windows Installer
- IBM Notes Client Version 8.5.3 oder 10.0 oder HCL Notes Client Version 11.0.1

  HINWEIS:

  - Führen Sie die Installation im Einzelbenutzermodus aus.
  - Es muss eine echte Installation durchgeführt werden. Während der Installation werden IBM Domino COM-Klassenbibliotheken registriert. Diese benötigt der IBM Notes Konnektor.
- Schreibzugriff auf das Installationsverzeichnis des IBM Notes Clients und auf das One Identity Manager Installationsverzeichnis.
- One Identity Manager Service, IBM Notes Konnektor
  - Installieren Sie die One Identity Manager Komponenten mit dem Installationsassistenten.
    1. Wählen Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen**.
    2. Wählen Sie die Maschinenrolle **Server | Jobserver | IBM Notes**.

Besondere Anforderungen für die Synchronisation einer IBM Domino 8.5 und 9 Umgebung

Für die Synchronisation einer IBM Domino 8.5 oder 9 Umgebung sind folgende minimale Versionen der IBM Notes und IBM Domino Komponenten erforderlich.

- IBM Domino Server in der Version 8.5.1 mit mindestens Fixpack 2 oder in der Version 9.0.1
- IBM Notes Client in der Version 8.5.3, Fixpack 4 oder IBM Notes Client in der Version 10.0

Um den Gateway Server einzurichten

1. Konfigurieren Sie den IBM Notes Client.

   Weitere Informationen finden Sie unter Um den IBM Notes Client zu konfigurieren auf Seite 19.
2. Installieren Sie den One Identity Manager Service und geben Sie den Gateway Server als Jobserver in der One Identity Manager-Datenbank bekannt. Weitere Informationen finden Sie unter Installation und Konfiguration des One Identity Manager Service auf Seite 21.

Um den IBM Notes Client zu konfigurieren

1. Erweitern Sie die PATH-Variable um den Standardsuchpfad (Installationsverzeichnis) und das Datenverzeichnis (`<Installationsverzeichnis>\Data`).

   In den Standardsuchpfad des Betriebssystems (PATH-Variable) ist der IBM Notes Installationspfad, das heißt der Pfad, in dem sich die `Notes.exe` befindet, einzutragen. Fügen Sie den bei der Installation des IBM Notes Clients gewählten Pfad zum Notes Datenverzeichnis ebenfalls zur PATH-Variablen hinzu.
2. Legen Sie die Verzeichnisse für die Ablage der ID-Dateien an (`<Installationsverzeichnis>\Data\IDS\<Name der Domäne>`).
3. Stellen Sie die Benutzer-ID-Datei des Synchronisationsbenutzers bereit.

   Es muss eine separate ID-Datei für diesen Benutzer bereitgestellt werden. Der Pfad zu dieser ID-Datei wird später in die kundenspezifische INI-Datei eingetragen. Benutzer-ID-Dateien mit Mehrfachkennwörtern werden nicht unterstützt.

   > HINWEIS: Es ist nicht die ID-Datei des Administrators zu benutzen, welche bei der Installation des Notes Servers erstellt wurde, da diese für andere administrative Tätigkeiten verwendet wird.
4. Halten Sie die Zertifizierer-ID-Dateien für zu verwaltende Zertifikate bereit.

   Stellen Sie auf dem Gateway Server alle Zertifizierer-ID-Dateien zur Verfügung, über die Benutzer registriert werden sollen. Zertifizierer-ID-Dateien mit Mehrfachkennwörtern werden nicht unterstützt.
5. Starten Sie den IBM Notes Client mit der ID-Datei des Synchronisationsbenutzers und melden Sie sich an.

Dadurch werden die Konfigurationseinträge auf dem Computer veranlasst. Zur Überprüfung der Zugriffsrechte kann mit der ID-Datei testweise ein neuer Benutzer gerechnet werden.

6. Kopieren Sie die Zertifikatsdokumente des Domino-Verzeichnisses in das persönliche Adressbuch des Benutzerkontos für die Synchronisation.
7. Prüfen Sie, ob die Zertifizierungsprotokoll-Datenbank `certlog.nsf` vorhanden ist.
8. Erstellen Sie eine kundendspezifische INI-Datei.

   Der Pfad zur ID-Datei des Synchronisationsbenutzers muss in dieser INI-Datei eingetragen werden.

HINWEIS:

- Wenn Sie den IBM Notes Client nicht im Standardinstallationsverzeichnis installiert haben, passen Sie die PATH-Variablen für den Standardsuchpfad und das Datenverzeichnis sowie die Pfadangaben in der `Notes.ini` und der kundenspezifischen INI-Datei an dieses Installationsverzeichnis an.
- Wenn Sie IBM Notes Client Version 10.0 nutzen, passen Sie die Pfadangabe zur `Notes.ini` an. Abhängig von der Installation kann diese Datei im Benutzerprofilverzeichnis gespeichert sein.

Detaillierte Informationen zum Thema

- Übernehmen der Notes Zertifikate auf Seite 20
- Erstellen einer kundenspezifischen INI-Datei auf Seite 20

Übernehmen der Notes Zertifikate

Bei der Einrichtung des Gateway Servers müssen die Zertifikatsdokumente aus dem Domino-Verzeichnis in das persönliche Adressbuch des Synchronisationsbenutzers kopiert werden. Das ist erforderlich, damit der IBM Notes Konnektor Benutzer in der Zielsystemumgebung anlegen, umbenennen oder verschieben kann.

TIPP: Übernehmen Sie neue Zertifikate regelmäßig aus dem Domino-Verzeichnis in das persönliche Adressbuch des Synchronisationsbenutzers. Ausführliche Informationen zum Kopieren von Zertifikatsdokumenten entnehmen Sie der Dokumentation Ihrer IBM Notes-Umgebung.

Erstellen einer kundenspezifischen INI-Datei

Bei der Konfiguration des IBM Notes Clients wird die Datei `Notes.ini` erzeugt. Diese Datei enthält verschiedene Konfigurationsinformationen, die der IBM Notes Konnektor für den Zugriff auf das Zielsystem benötigt. Erstellen Sie eine Kopie dieser INI-Datei und stellen Sie diese als kundenspezifische INI-Datei dem IBM Notes Konnektor zur Verfügung. Die kundenspezifische INI-Datei muss den Pfad zur ID-Datei des Synchronisationsbenutzers

enthalten. Bei der Konfiguration der Systemverbindung mit dem Synchronization Editor geben Sie diese INI-Datei und das Kennwort der Benutzer-ID-Datei an.

Um eine kundenspezifische INI-Datei anzulegen

1. Erstellen Sie eine Kopie der Datei `Notes.ini`. Verwenden Sie dafür die ID-Datei des Synchronisationsbenutzers.
2. Prüfen Sie in der Kopie die folgenden Werte.

Tabelle 4: Benötigte Parameter in der kundenspezifischen INI-Datei

Parameter	Beschreibung
Directory	Pfad auf das Notes-Datenverzeichnis (lokales Verzeichnis).
KeyFileName	Pfad zur ID-Datei des Synchronisationsbenutzers (lokales Verzeichnis).
KitType	Notes Typ: 1 = Client, 2 = Server.

Installation und Konfiguration des One Identity Manager Service

Der Gateway Server übernimmt die Funktion des 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. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein.

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 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.
- Remote-Installation der One Identity Manager Service-Komponenten entsprechend der Maschinenrollen.
- Konfigurieren des One Identity Manager Service.
- Starten des One Identity Manager Service.

HINWEIS: 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 Einrichten des Jobservers finden Sie im *One Identity Manager Konfigurationshandbuch*.

HINWEIS: Das Programm führt eine Remote-Installation des One Identity Manager Service aus. Eine lokale Installation des Dienstes ist mit diesem Programm nicht möglich. Die Remote-Installation wird nur innerhalb einer Domäne oder in Domänen mit Vertrauensstellung unterstützt.

Für die Remote-Installation des One Identity Manager Service benötigen Sie eine administrative Arbeitsstation, auf der die One Identity Manager-Komponenten installiert sind. Ausführliche Informationen zur Installation einer Arbeitsstation finden Sie im *One Identity Manager Installationshandbuch*.

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

1. Starten Sie das Programm Server Installer auf Ihrer administrativen Arbeitsstation.
2. Auf der Seite **Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.
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 zur 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 One Identity Manager Service 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 **IBM Notes**.
5. Auf der Seite **Serverfunktionen** wählen Sie **IBM Notes 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 **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.
   - Für eine Verbindung zum Anwendungsserver:
     a. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
     b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     c. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.
     d. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
     e. Wählen Sie das Authentifizierungsmodul. 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*.
7. Zur Konfiguration der Remote-Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** wählen Sie das Verzeichnis mit den Installationsdateien.
10. Auf der Seite **Datenbankschlüsseldatei auswählen** wählen die Datei mit dem privaten Schlüssel.

    HINWEIS: Diese Seite wird nur angezeigt, wenn die Datenbank verschlüsselt ist.
11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
    - **Computer**: Name oder IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
    - **Dienstkonto**: Angaben zum Benutzerkonto des One Identity Manager Service.
      - Um den Dienst unter dem Konto **NT AUTHORITY\SYSTEM** zu starten, aktivieren Sie die Option **Lokales Systemkonto**.

- Um den Dienst unter einem anderen Konto zu starten, deaktivieren Sie die Option **Lokales Systemkonto** und erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung.

- **Installationskonto**: Angaben zum administrativen Benutzerkonto für die Installation des Dienstes.
  - Um das Benutzerkonto des angemeldeten Benutzers zu verwenden, aktivieren Sie die Option **Angemeldeter Benutzer**.
  - Um ein anderes Benutzerkonto zu verwenden, deaktivieren Sie die Option **Angemeldeter Benutzer** und geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.
- Um das Installationsverzeichnis, den Namen, den Anzeigenamen oder die Beschreibung für den One Identity Manager Service zu ändern, nutzen Sie die weiteren Optionen.

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

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

13. 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.

Anlegen einer Archivdatenbank zur Sicherung der Personendokumente

Um Benutzer-ID-Dateien über das ID-Restore-Verfahren wiederherstellen zu können, legen Sie eine Archivdatenbank zur Sicherung der ID-Dateien an. Beim Anlegen eines neuen Benutzerkontos im One Identity Manager wird eine Kopie des initialen Personendokuments in eine Archivdatenbank auf dem Gateway Server kopiert. Diese Archivdatenbank muss initial angelegt werden und sollte Bestandteil des täglichen Backups sein.

HINWEIS: Die Archivdatenbank wird nur benötigt, wenn an der Domäne die Option **ID-Vault aktiv** deaktiviert ist und wenn Benutzer-ID-Dateien über den One Identity Manager wiederherstellbar sein sollen. Weitere Informationen finden Sie unter ID-Restore auf Seite 139.

Die schnellste Möglichkeit eine Archivdatenbank einzurichten, ist die Erstellung einer leere Kopie des lokalen Adressbuchs auf dem Gateway Server.

Tabelle 5: Benötigte Daten für die Kopie

Eigenschaft	Wert
Server	Lokal

Eigenschaft	Wert
Titel	beliebige Bezeichnung
Dateiname	`Archive.nsf`
Nur Anwendungsgestaltung	aktiviert

Standardmäßig wird die Kopie des lokalen Adressbuchs für den angemeldeten Benutzer verschlüsselt. Damit der IBM Notes Konnektor auf die Archivdatenbank zugreifen kann, muss die Kopie des lokalen Adressbuchs für Synchronisationsbenutzer verschlüsselt werden.

Ausführliche Informationen zum Anlegen der Adressbuchkopie entnehmen Sie der Dokumentation Ihrer IBM Notes-Umgebung.

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Notes Domäne

Verwenden Sie den Synchronization Editor, um die Synchronisation zwischen One Identity Manager-Datenbank und IBM Notes-Umgebung einzurichten. Nachfolgend sind die Schritte für die initiale Einrichtung eines Synchronisationsprojektes beschrieben.

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.

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

Tabelle 6: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Domino-Server	Name des Domino-Servers, mit dem der Gateway Server kommuniziert.
Domino-Verzeichnis	Name des Domino-Verzeichnisses (`Names.nsf`).
Kundenspezifische INI-Datei	Name und Pfad zur kundenspezifischen INI-Datei. Weitere Informationen finden Sie unter Erstellen einer kundenspezifischen INI-Datei auf Seite 20.

Angaben	Erläuterungen
Kennwort der ID-Datei	Kennwort der ID-Datei des Synchronisationsbenutzers. Der Pfad zu dieser ID-Datei muss in der kundenspezifischen INI-Datei angegeben sein. Über den Synchronisationsbenutzer greift der IBM Notes Konnektor auf das Zielsystem zu. Stellen Sie einen Benutzer mit ausreichenden Berechtigungen bereit. Weitere Informationen finden Sie unter Benutzer und Berechtigungen für die Synchronisation mit einer IBM Notes-Umgebung auf Seite 16.
Synchronisationsserver	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. Der Gateway Server übernimmt die Funktion des Synchronisationsservers. Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem IBM Notes Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften. **Tabelle 7: Zusätzliche Eigenschaften für den Jobserver** **Eigenschaft** / **Wert** Serverfunktion / IBM Notes Konnektor Maschinenrolle / Server/Jobserver/IBM Notes Weitere Informationen finden Sie unter Installation und Konfiguration des One Identity Manager Service auf Seite 21.
Verbindungsdaten zur One Identity Manager-Datenbank	• Datenbankserver • Datenbank • SQL Server Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.

Angaben	Erläuterungen
Remoteverbindungsserver	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 Synchronization Editor nicht direkt auf dem Gateway Server gestartet werden kann, kann eine Remoteverbindung eingerichtet werden. ***Um eine Remoteverbindung zu nutzen*** 1. Stellen Sie eine Arbeitsstation bereit, auf der der Synchronization Editor installiert ist. 2. Installieren Sie das **RemoteConnectPlugin** auf dem Gateway Server. Damit übernimmt der Gateway Server gleichzeitig die Funktion des Remoteverbindungsservers. 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 • IBM Notes Konnektor ist installiert Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt. Ausführliche Informationen zum Herstellen einer Remoteverbindung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

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.

Um ein initiales Synchronisationsprojekt für eine Notes Domäne einzurichten

1. Starten Sie das Launchpadauf dem Gateway Server 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 IBM Notes** 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.
   - Haben Sie das Launchpad auf dem Gateway Server gestartet, nehmen Sie keine Einstellungen vor.
   - Haben Sie das Launchpad auf einer Arbeitsstation gestartet, stellen Sie eine Remoteverbindung her.

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

4. Auf der Seite **Verbindungsdaten zum IBM Domino Verzeichnis** erfassen Sie die Verbindungsparameter, die der IBM Notes Konnektor zur Anmeldung am Zielsystem benötigt.

   Tabelle 8: Verbindungsdaten zum Domino-Server

Eigenschaft	Beschreibung
INI-Datei	Name und Pfad zur kundenspezifischen INI-Datei.
Domino-Server	Name des Domino-Servers, mit dem der Gateway Server kommuniziert.
Domino-Verzeichnis	Name des Domino-Verzeichnisses (`Names.nsf`).
Kennwort der ID-Datei	Kennwort der ID-Datei des Synchronisationsbenutzers. Der Pfad zu dieser ID-Datei muss in der kundenspezifischen INI-Datei angegeben sein.

5. Auf der Seite **Verbindungseinstellungen prüfen** können Sie die erfassten Verbindungsdaten überprüfen. Klicken Sie **Jetzt prüfen**.

   Der One Identity Manager versucht eine Verbindung zum Zielsystem aufzubauen.

6. Auf der Seite **Konfigurationseinstellungen** können Sie zusätzliche Einstellungen vornehmen.
   - Um Notes Objekte über AdminP-Prozesse löschen zu können, aktivieren Sie **Objekte über AdminP-Prozesse löschen**. Wenn die Option deaktiviert ist, werden die Objekte im Zielsystem durch den IBM Notes Konnektor direkt gelöscht.

- 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 9: Zielsystemzugriff festlegen

Option	Bedeutung
Das Zielsystem soll nur eingelesen werden.	Angabe, 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.	Angabe, 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.

    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**.

    HINWEIS: 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.

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

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Um das Synchronisationsprotokoll für die Zielsystemverbindung zu konfigurieren, wählen Sie die Kategorie **Konfiguration | Zielsystem**.
3. Um das Synchronisationsprotokoll für die Datenbankverbindung zu konfigurieren, wählen Sie die Kategorie **Konfiguration | One Identity Manager Verbindung**.
4. Wählen Sie den Bereich **Allgemein** und klicken Sie **Konfigurieren**.
5. Wählen Sie den Bereich **Synchronisationsprotokoll** und aktivieren Sie **Synchronisationsprotokoll erstellen**.

6. 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.

7. Klicken Sie **OK**.

Um regelmäßige Synchronisationen auszuführen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
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**.

Um die initiale Synchronisation manuell zu starten

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
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**.

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 Domäne 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.

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie der Domäne 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 **IBM Notes | Benutzerkonten | Verbunden aber nicht konfiguriert | <Domäne>**.
   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

- One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation

Verwandte Themen

- Installation und Konfiguration eines Gateway Servers auf Seite 18
- Benutzer und Berechtigungen für die Synchronisation mit einer IBM Notes-Umgebung auf Seite 16
- Synchronisationsergebnisse anzeigen auf Seite 32
- Anpassen einer Synchronisationskonfiguration auf Seite 33
- Beschleunigung der Synchronisation durch Revisionsfilterung auf Seite 37
- Nutzung von AdminP-Aufträgen zur Verarbeitung von IBM Notes Prozessen auf Seite 200
- Standardprojektvorlage für IBM Notes auf Seite 211
- Einrichten von Kontendefinitionen auf Seite 47
- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 129

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 das Synchronisationsprojekt im Synchronization Editor.
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 das Synchronisationsprojekt im Synchronization Editor.
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.

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.

Anpassen einer Synchronisationskonfiguration

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation einer Notes Domäne eingerichtet. Mit diesem Synchronisationsprojekt können Sie Notes Objekte in die One Identity Manager-Datenbank einlesen. Wenn Sie Benutzerkonten und ihre Berechtigungen mit dem One Identity Manager verwalten, werden Änderungen in die IBM Notes-Umgebung provisioniert.

Um die Datenbank und die IBM Notes-Umgebung regelmäßig abzugleichen und Änderungen zu synchronisieren, passen Sie die Synchronisationskonfiguration an.

- Um bei der Synchronisation den One Identity Manager als Mastersystem zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um festzulegen, welche Notes 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 Domänen eingerichtet werden. Hinterlegen Sie die Verbindungsparameter zur Anmeldung an den Domänen 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.

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.

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

Detaillierte Informationen zum Thema

- Synchronisation in die IBM Notes-Umgebung konfigurieren auf Seite 34
- Synchronisation verschiedener Notes Domänen konfigurieren auf Seite 35
- Schema aktualisieren auf Seite 36

Synchronisation in die IBM Notes-Umgebung 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

Mastersystem zu nutzen, benötigen Sie zusätzlich einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.

Um eine Synchronisationskonfiguration für die Synchronisation in die IBM Notes-Umgebung zu erstellen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
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 Notes Domänen konfigurieren auf Seite 35

Synchronisation verschiedener Notes Domänen konfigurieren

Voraussetzungen

- Die Zielsystemschemas beider Domänen sind identisch.
- Alle virtuellen Schemaeigenschaften, die im Mapping genutzt werden, müssen in den erweiterten Schemas beider Domänen vorhanden sein.

Um ein Synchronisationsprojekt für die Synchronisation einer weiteren Domäne anzupassen

1. Stellen Sie in der weiteren Domäne einen Synchronisationsbenutzer mit ausreichenden Berechtigungen bereit.
2. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
3. Erstellen Sie für die weitere Domäne ein neues Basisobjekt. Verwenden Sie den Assistenten zur Anlage eines Basisobjektes.
   - Wählen Sie im Assistenten den IBM Notes Konnektor und 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 die IBM Notes-Umgebung konfigurieren auf Seite 34
- Benutzer und Berechtigungen für die Synchronisation mit einer IBM Notes-Umgebung auf Seite 16

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 das Synchronisationsprojekt im Synchronization Editor.
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 das Synchronisationsprojekt im Synchronization Editor.
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

Beim Start der Synchronisation werden alle zu synchronisierenden Objekte geladen. Ein Teil dieser Objekte wurde gegebenenfalls seit der letzten Synchronisation nicht geändert und muss daher bei der Synchronisation nicht verarbeitet werden. Indem nur solche Objekte geladen werden, die sich seit der letzten Synchronisation geändert haben, kann die Synchronisation beschleunigt werden. Zur Beschleunigung der Synchronisation nutzt der One Identity Manager die Revisionsfilterung.

IBM Notes unterstützt die Revisionsfilterung. Als Revisionszähler wird das Datum der letzten Änderung der Notes Dokumente genutzt. Jede Synchronisation speichert ihr letztes Ausführungsdatum als Revision in der One Identity Manager-Datenbank (Tabelle `DPRRevisionStore`, Spalte `Value`). Dieser Wert wird als Vergleichswert für die Revisionsfilterung bei der nächsten Synchronisation mit dem selben Workflow genutzt. Bei der Synchronisation mit diesem Workflow wird das Änderungsdatum der Notes Objekte mit der in der One Identity Manager-Datenbank gespeicherten Revision verglichen. Es werden nur noch die Objekte aus dem Zielsystem gelesen, die sich seit diesem Datum verändert haben.

Die Revision wird zu Beginn einer Synchronisation ermittelt. Objekte, die durch die Synchronisation geändert werden, werden bei der nächsten Synchronisation nochmals

geladen und überprüft. Die zweite Synchronisation nach der Initialsynchronisation ist daher noch nicht deutlich schneller.

Die Revisionsfilterung kann an den Workflows oder an den Startkonfigurationen zugelassen werden.

Um die Revisionsfilterung an einem Workflow zuzulassen

- Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
- Bearbeiten Sie die Eigenschaften des Workflows. Wählen Sie in der Auswahlliste **Revisionsfilterung** den Eintrag **Revisionsfilter nutzen**.

Um die Revisionsfilterung an einer Startkonfiguration zuzulassen

- Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
- Bearbeiten Sie die Eigenschaften der Startkonfiguration. Wählen Sie in der Auswahlliste **Revisionsfilterung** den Eintrag **Revisionsfilter nutzen**.

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

HINWEIS: Der IBM Notes Konnektor kann die Datumsinformationen nur aus den Notes Dokumenten auslesen, wenn auf dem Domino-Server ein Volltextindex für das Domino-Verzeichnis eingerichtet ist.

Nachbehandlung ausstehender Objekte

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 **IBM Notes | Zielsystemabgleich: IBM Notes**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp **IBM Notes** 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

a. Wählen Sie auf dem Formular für den Zielsystemabgleich das Objekt.

b. 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 10: 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. Die Markierung **Ausstehend** wird für das Objekt entfernt. Indirekte Mitgliedschaften können nicht gelöscht werden.
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung **Ausstehend** wird für das Objekt entfernt. Die Methode löst das Ereignis `HandleOutstanding` aus. Dadurch wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt.

Symbol	Methode	Beschreibung
		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 .

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 **IBM Notes | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **IBM Notes**.
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.

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.

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.
- 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 **IBM Notes | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **IBM Notes**.
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.
    - Die Option kann nur für Zuordnungstabellen aktiviert werden, deren Basistabelle eine Spalte `XDateSubItem` oder `CCC_XDateSubItem` hat.
    - Zuordnungstabellen, die im Mapping in einer virtuellen Schemaeigenschaft zusammengefasst sind, müssen identisch markiert werden.
5. Klicken Sie **Merge-Modus**.
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. 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 Icon gekennzeichnet:  . Die originale Bedingung kann jederzeit wiederhergestellt werden.

Um die Standardbedingung 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.

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

Beschleunigung der Einzelobjektsynchronisation

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

Die Lastverteilung wird nicht für Provisionierungsprozesse in die IBM Notes-Umgebung genutzt, um zu verhindern, dass durch die parallele Verarbeitung inkonsistente Daten im Zielsystem entstehen. Keine Lastverteilung erfolgt, wenn die Anzahl der maximalen Instanzen an der Prozessfunktion oder Prozesskomponente auf **1** oder **-1** gesetzt ist.

HINWEIS: Die Lastverteilung sollte nicht permanent für 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 Einzelobjektsynchronisation ausführt.

Um die Lastverteilung zu konfigurieren

1. Konfigurieren Sie die Server und geben Sie diese im One Identity Manager als Jobserver bekannt.
   - Weisen Sie diesen Jobservern die Serverfunktion **IBM Notes Konnektor** zu.

   Alle Jobserver müssen auf die gleiche Notes Domäne 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 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 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

- Bearbeiten eines Servers auf Seite 79

Unterstützung bei der Analyse von Synchronisationsproblemen

Für die Analyse von Problemen während der Synchronisation, beispielsweise unzureichender Performance, kann ein Bericht erzeugt werden. Der Bericht enthält Informationen wie beispielsweise:

- Ergebnisse der Konsistenzprüfung
- Einstellungen zur Revisionsfilterung
- Verwendeter Scope
- Analyse des Synchronisationspuffers
- Zugriffszeiten auf die Objekte in der One Identity Manager-Datenbank und im Zielsystem

Um den Synchronisationsanalysebericht zu erstellen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie das Menü **Hilfe | Synchronisationsanalysebericht erstellen** und beantworten Sie die Sicherheitsabfrage mit **Ja**.

   Die Generierung des Berichts nimmt einige Zeit in Anspruch. Er wird in einem separaten Fenster angezeigt.
3. Drucken Sie den Bericht oder Speichern Sie ihn in einem der verschiedenen Ausgabeformate.

Deaktivieren der Synchronisation

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

Um regelmäßige Synchronisationen zu verhindern

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

Detaillierte Informationen zum Thema

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Notes Domäne auf Seite 25

3

Basisdaten zur Konfiguration

Für die Verwaltung einer IBM Notes-Umgebung im One Identity Manager sind folgende Basisdaten relevant.

- Konfigurationsparameter

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

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

  Weitere Informationen finden Sie unter Konfigurationsparameter für die Synchronisation mit einer Notes Domäne auf Seite 206.

- Kontendefinitionen

  Um im laufenden Betrieb 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 Einrichten von Kontendefinitionen auf Seite 47.

- 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 Notes Benutzerkonten auf Seite 65.

- Initiales Kennwort für neue Benutzerkonten

  Um das initiale Kennwort für Benutzerkonten zu vergeben, stehen Ihnen verschiedene Möglichkeiten zur Verfügung. Es kann das zentrale Kennwort der zugeordneten Person auf das Kennwort des Benutzerkontos abgebildet werden, es kann ein fest vorgegebenes Kennwort verwendet werden oder ein zufällig generiertes initiales Kennwort vergeben werden.

  Weitere Informationen finden Sie unter Initiales Kennwort für neue Notes Benutzerkonten auf Seite 76.

- E-Mail-Benachrichtigungen über die Anmeldeinformationen

  Bei Erstellung eines neuen Benutzerkontos werden die Anmeldeinformationen an definierte Empfänger versendet. Dabei werden zwei Benachrichtigungen versendet, die den Benutzernamen und das initiale Kennwort enthalten. Zur Erzeugung der Benachrichtigungen werden Mailvorlagen genutzt.

  Weitere Informationen finden Sie unter E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 78.

- Zielsystemtypen

  Zielsystemtypen werden für die Konfiguration des Zielsystemabgleichs benötigt. An den Zielsystemtypen werden die Tabellen gepflegt, die ausstehende Objekte enthalten können.

  Weitere Informationen finden Sie unter Nachbehandlung ausstehender Objekte auf Seite 38.

- Zielsystemverantwortliche

  Im One Identity Manager ist eine Standardanwendungsrolle für die Zielsystemverantwortlichen vorhanden. Weisen Sie dieser Anwendungsrolle die Personen zu, die berechtigt sind, alle Domänen im One Identity Manager zu bearbeiten.

  Wenn Sie die Bearbeitungsrechte der Zielsystemverantwortlichen auf einzelne Domänen einschränken wollen, definieren Sie weitere Anwendungsrollen. Die Anwendungsrollen müssen der Standardanwendungsrolle untergeordnet sein.

  Weitere Informationen finden Sie unter Zielsystemverantwortliche auf Seite 85.

- Server

  Für die Verarbeitung der IBM Notes spezifischen Prozesse im One Identity Manager müssen die Server mit ihren Serverfunktionen bekannt sein. Dazu gehört beispielsweise der Gateway Server.

  Weitere Informationen finden Sie unter Bearbeiten eines Servers auf Seite 79.

Einrichten von Kontendefinitionen

Um im laufenden Betrieb 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.

Ausführliche Informationen zu Kontendefinitionen finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

- Erstellen einer Kontendefinition
- Erstellen der Automatisierungsgrade
- Erstellen einer Abbildungsvorschrift für IT Betriebsdaten
- Erfassen der IT Betriebsdaten
- Zuweisen der Kontendefinition an Personen
- (Optional) Zuweisen der Kontendefinition an ein Zielsystem

Erstellen einer Kontendefinition

Um eine Kontendefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **IBM Notes | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

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

Stammdaten einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 11: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte Kontendefinition	Vorausgesetzte Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch mitbestellt oder zugeordnet. Für eine IBM Notes Domäne lassen Sie die Angabe leer.
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. Erfassen Sie einen Wert zwischen 0 und 1. 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	Angabe, 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	Angabe, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von den Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig.

Eigenschaft	Beschreibung
Automatische Zuweisung zu Personen	Angabe, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Beim Speichern wird die Kontendefinition an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine Person neu angelegt wird, erhält sie ebenfalls automatisch diese Kontendefinition. WICHTIG: Aktivieren Sie diese Option nur, 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 die automatische Zuweisung der Kontendefinition an alle Personen zu entfernen, deaktivieren Sie die Option. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.
Kontendefinition bei dauerhafter Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: 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: 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: 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: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.

Eigenschaft	Beschreibung
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.

Erstellen der Automatisierungsgrade

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

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 Automatisierungsgrade an eine Kontendefinition zuzuweisen

1. Wählen Sie im Manager die Kategorie **IBM Notes | 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.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Automatisierungsgrade.
5. Speichern Sie die Änderungen.

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

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie im Manager die Kategorie **IBM Notes | Basisdaten zur Konfiguration | Kontendefinitionen | Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

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

Stammdaten eines Automatisierungsgrades

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 12: Stammdaten eines Automatisierungsgrades

Eigenschaft	Beschreibung
Automatisierungsgrad	Bezeichnung des Automatisierungsgrades.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Betriebsdaten überschreibend	Angabe, ob Daten an Benutzerkonten, die sich aus den IT Betriebsdaten bilden, automatisch aktualisiert werden. Zulässige Werte sind: • **Niemals**: Die Daten werden nicht aktualisiert. • **Immer**: Die Daten werden immer aktualisiert. • **Nur initial**: Die Daten werden nur initial ermittelt.
Gruppen bei zeitweiliger Deaktivierung beibehalten	Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei zeitweiliger Deaktivierung sperren	Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen gesperrt werden sollen.
Gruppen bei dauerhafter Deaktivierung beibehalten	Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei dauerhafter Deaktivierung sperren	Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen gesperrt werden sollen.
Gruppen bei verzögertem Löschen beibehalten	Angabe, ob die Benutzerkonten zum Löschen markierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei verzögertem Löschen sperren	Angabe, ob die Benutzerkonten zum Löschen markierter Personen gesperrt werden sollen.
Gruppen bei Sicherheitsgefährdung beibehalten	Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei Sicherheitsgefährdung sperren	Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen gesperrt werden sollen.
Gruppen bei deaktiviertem Benutzerkonto beibehalten	Angabe, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen.

Erstellen einer Abbildungsvorschrift für IT Betriebsdaten

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.

- IBM Notes Server
- IBM Notes Zertifikat
- Schablone für Postfachdatei
- Gruppen erbbar
- Identität
- Privilegiertes Benutzerkonto

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

1. Wählen Sie im Manager die Kategorie **IBM Notes | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **IT Betriebsdaten Abbildungsvorschrift bearbeiten** und erfassen Sie folgende Informationen.

Tabelle 13: Abbildungsvorschrift für IT Betriebsdaten

Eigenschaft	Beschreibung
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: Verwenden Sie die primäre Geschäftsrolle

Eigenschaft	Beschreibung
	nur, 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	Angabe, 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	Angabe, 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 den Konfigurationsparameter **TargetSystem | NDO | Accounts | MailTemplateDefaultValues** an.

4. Speichern Sie die Änderungen.

Erfassen der IT Betriebsdaten

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 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 Domäne A. Zusätzlich erhalten einige Personen der Abteilung A administrative Benutzerkonten in der Domäne A.

Erstellen Sie eine Kontendefinition A für die Standardbenutzerkonten der Domäne A und eine Kontendefinition B für die administrativen Benutzerkonten der Domäne 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 Domäne 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.

Tabelle 14: IT Betriebsdaten

Eigenschaft	Beschreibung
Wirksam für	Anwendungsbereich der IT Betriebsdaten. 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	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	Konkreter Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.

4. Speichern Sie die Änderungen.

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, Geschäftsrolle oder zu einem primären Standort, werden die Bildungsregeln automatisch ausgeführt.

Um die Bildungsregeln auszuführen

1. Wählen Sie im Manager die Kategorie **IBM Notes | 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.

Alter Wert:	Aktueller Wert der Objekteigenschaft.
Neuer Wert:	Wert, den die Objekteigenschaft durch die Änderung an den IT Betriebsdaten annehmen würde.
Auswahl:	Angabe, ob die Änderung 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 Kontendefinition 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.

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.

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.

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

Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **IBM Notes | 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.

Kontendefinition an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **IBM Notes | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** 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.

Kontendefinition an alle Personen zuweisen

Um eine Kontendefinition an alle Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **IBM Notes | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.

   WICHTIG: Aktivieren Sie diese Option nur, 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!
5. Speichern Sie die Änderungen.

Die Kontendefinition wird an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine Person neu angelegt wird, erhält sie ebenfalls automatisch diese Kontendefinition. Die Zuweisung wird durch den DBQueue Prozessor berechnet.

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

Kontendefinition direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **IBM Notes | 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.

Kontendefinition an Systemrollen zuweisen

Installierte Module: Systemrollenmodul

HINWEIS: 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 **IBM Notes | 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.

Kontendefinition 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

1. Wählen Sie im Manager die Kategorie **IBM Notes | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen** (bei rollenbasierter Anmeldung).
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

1. Wählen Sie im Manager die Kategorie **IBM Notes | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen** (bei rollenbasierter Anmeldung).
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

1. Wählen Sie im Manager die Kategorie **IBM Notes | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen** (bei rollenbasierter Anmeldung).
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 einer Kontendefinition auf Seite 48
- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 58
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 59
- Kontendefinition direkt an Personen zuweisen auf Seite 60
- Kontendefinition an Systemrollen zuweisen auf Seite 60

Zuweisen der Kontendefinition an ein Zielsystem

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 **IBM Notes | Domäne** die Domäne.
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.

Löschen einer Kontendefinition

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 **IBM Notes | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Deaktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.
    e. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Personen.
    a. Wählen Sie im Manager die Kategorie **IBM Notes | 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 **IBM Notes | 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 **IBM Notes | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

   d. 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 Anwenderhandbuch für das Web Portal*.

   Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

   a. Wählen Sie im Manager die Kategorie **IBM Notes | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

      - ODER -

      Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen** (bei rollenbasierter Anmeldung).

   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 **IBM Notes | 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 **IBM Notes | Domäne** die Domäne.
   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 **IBM Notes | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
   b. Wählen Sie in der Ergebnisliste die Kontendefinition.
   c. Klicken Sie , um die Kontendefinition zu löschen.

Kennwortrichtlinien für Notes Benutzerkonten

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 66
- Anwenden einer Kennwortrichtlinie auf Seite 67
- Bearbeiten von Kennwortrichtlinien auf Seite 69
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 72
- Ausschlussliste für Kennwörter auf Seite 75
- Prüfen eines Kennwortes auf Seite 75
- Generieren eines Kennwortes testen auf Seite 76

Vordefinierte Kennwortrichtlinien

Die vordefinierte 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.

HINWEIS: Bei der Aktualisierung von One Identity Manager Version 7.x auf One Identity Manager Version 8.1.4 werden die Einstellung der Konfigurationsparameter zur Bildung von Kennwörtern auf die zielsystemspezifischen Kennwortrichtlinien umgesetzt.

Für Notes ist die Kennwortrichtlinie **IBM Notes Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Notes Benutzerkonten (`NDOUser.UserPassword`, `NDOUser.InternetPassword` und `NDOUser.InitialPassword`) einer Notes Domäne anwenden.

Wenn die Kennwortanforderungen der Domänen unterschiedlich sind, wird empfohlen, je Domäne eine eigene Kennwortrichtlinie einzurichten.

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

Anwenden einer Kennwortrichtlinie

Für Notes ist die Kennwortrichtlinie **IBM Notes Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Notes Benutzerkonten (`NDOUser.UserPassword`, `NDOUser.InternetPassword` und `NDOUser.InitialPassword`) einer Notes Domäne anwenden.

Wenn die Kennwortanforderungen der Domänen unterschiedlich sind, wird empfohlen, je Domäne 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. Kennwortrichtlinien der Notes Domäne des Benutzerkontos
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 **IBM Notes | 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.

Tabelle 15: Zuweisen einer Kennwortrichtlinie

Eigenschaft	Beschreibung
Anwenden auf	Anwendungsbereich der Kennwortrichtlinie. ***Um den Anwendungsbereich festzulegen*** a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. b. 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`. c. 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. d. 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 **IBM Notes | 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.

Bearbeiten von Kennwortrichtlinien

Um eine Kennwortrichtlinie zu bearbeiten

1. Wählen Sie im Manager die Kategorie **IBM Notes | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie und wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Kennwortrichtlinie auf Seite 69
- Richtlinieneinstellungen auf Seite 70
- Zeichenklassen für Kennwörter auf Seite 71
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 72

Allgemeine Stammdaten einer Kennwortrichtlinie

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 16: 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 .

Eigenschaft	Bedeutung
Eigentümer (Anwendungsrolle)	Anwendungsrolle, deren Mitglieder die Kennwortrichtlinie konfigurieren können.
Standardrichtlinie	Kennzeichnung als Standardrichtlinie für Kennwörter. 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 17: Richtlinieneinstellungen

Eigenschaft	Bedeutung
Initiales Kennwort	Initiales Kennwort für neu erzeugte Benutzerkonten. Wird beim Erstellen eines Benutzerkontos kein Kennwort angegeben oder kein Zufallskennwort generiert, dann wird das initiale Kennwort benutzt.
Kennwortbestätigung	Kennwortwiederholung.
Min. Länge	Minimale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben muss.
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. Wird nur berücksichtigt, bei Anmeldung am One Identity Manager. 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 erreicht, 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 Anwenderhandbuch für das Web Portal*.

Eigenschaft	Bedeutung
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.
Kennwortchronik	Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert **5** eingegeben, werden die letzten fünf Kennwörter des Benutzers gespeichert.
Min. Kennwortstärke	Angabe, 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	Angabe, 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 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 18: Zeichenklassen für Kennwörter

Eigenschaft	Bedeutung
Min. Anzahl Buchstaben	Angabe, wie viele alphabetische Zeichen ein Kennwort mindestens enthalten muss.
Min. Anzahl Kleinbuchstaben	Angabe, wie viele Kleinbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Großbuchstaben	Angabe, wie viele Großbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Ziffern	Angabe, wie viele Ziffern ein Kennwort mindestens enthalten muss.
Min. Anzahl Sonderzeichen	Angabe, wie viele Sonderzeichen ein Kennwort mindestens enthalten muss.

Eigenschaft	Bedeutung
Zulässige Sonderzeichen	Liste zulässiger Sonderzeichen.
Max. identische Zeichen insgesamt	Maximale Anzahl identischer Zeichen, die insgesamt im Kennwort vorkommen dürfen.
Max. identische Zeichen aufeinanderfolgend	Maximale Anzahl identischer Zeichen, die nacheinander wiederholt werden können.
Unzulässige Sonderzeichen	Liste unzulässiger Sonderzeichen.
Keine Kleinbuchstaben erzeugen	Angabe, ob ein generiertes Kennwort Kleinbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keinen Großbuchstaben erzeugen	Angabe, ob ein generiertes Kennwort Großbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keine Ziffern erzeugen	Angabe, ob ein generiertes Kennwort Ziffern enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keine Sonderzeichen erzeugen	Angabe, 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 73
- Skript zum Generieren eines Kennwortes auf Seite 74

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 für ein 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 **IBM Notes | 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 74

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 für ein 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 **IBM Notes | 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 73

Ausschlussliste für Kennwörter

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.

Prüfen eines Kennwortes

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 **IBM Notes | 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 eines Kennwortes 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 **IBM Notes | 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 Notes Benutzerkonten

Tabelle 19: Konfigurationsparameter für die Bildung eines initialen Kennwortes für Benutzerkonten

Konfigurationsparameter	Bedeutung
QER\Person\UseCentralPassword	Der Konfigurationsparameter legt fest, ob das zentrale Kennwort einer Person in den

Konfigurationsparameter	Bedeutung
	Benutzerkonten verwendet werden soll. Das zentrale Kennwort der Person wird automatisch auf die Benutzerkonten der Person in allen erlaubten Zielsystemen abgebildet. Ausgenommen sind privilegierte Benutzerkonten; diese werden nicht aktualisiert.
QER\Person\UseCentralPassword\PermanentStore	Der Konfigurationsparameter steuert die Aufbewahrungszeit der zentralen Kennworte. Ist der Konfigurationsparameter aktiviert, wird das zentrale Kennwort in der One Identity Manager-Datenbank gespeichert und wird für neue Benutzerkonten genutzt. Ist der Konfigurationsparameter deaktiviert, wird das zentrale Kennwort nach dem Publizieren an die bestehenden Benutzerkonten aus der One Identity Manager-Datenbank gelöscht werden. Das zentrale Kennwort steht für weitere Benutzerkonten nicht zur Verfügung.
TargetSystem\NDO\Accounts\InitialRandomPassword	Der Konfigurationsparameter legt fest, 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\NDO\MinPasswordLength	Angabe der minimalen Kennwortlänge, die in allen neu zu berechnenden Notes ID-Dateien zu setzen ist.

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

- Erstellen Sie Benutzerkonten manuell und tragen Sie in den Stammdaten der Benutzerkonten ein Kennwort ein.
- Vergeben Sie beim Erstellen von Benutzerkonten ein zufällig generiertes initiales Kennwort.
  - Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | NDO | 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.
- Verwenden Sie das zentrale Kennwort der Person. Das zentrale Kennwort der zugeordneten Person wird auf das Kennwort des Benutzerkontos abgebildet. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- Kennwortrichtlinien für Notes Benutzerkonten auf Seite 65
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 78

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:

1. Stellen Sie sicher, dass das E-Mail-Benachrichtungssystem im One Identity Manager konfiguriert ist. Ausführliche Informationen finden Sie im *One Identity Manager Installationshandbuch*.
2. Aktivieren Sie im Designer den Konfigurationsparameter **Common | MailNotification | DefaultSender** und geben Sie die Absenderadresse an, mit der die E-Mail Benachrichtigungen verschickt werden.
3. Stellen Sie sicher, dass alle Personen eine Standard-E-Mail-Adresse besitzen. An diese E-Mail Adresse werden die Benachrichtigungen versendet. Ausführliche

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

4. Stellen Sie sicher, dass für alle Personen eine Sprachkultur ermittelt werden kann. Nur so erhalten die Personen die E-Mail Benachrichtigungen in ihrer Sprache. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

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

Bearbeiten eines Servers

Für die Verarbeitung der IBM Notes-spezifischen Prozesse im One Identity Manager muss der Gateway Server 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 **IBM Notes | Basisdaten zur Konfiguration | Server** einen Eintrag für den Jobserver 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.

HINWEIS: Damit ein Server seine Funktion im One Identity Manager Netzwerk ausführen kann, muss ein One Identity Manager Service installiert, konfiguriert und gestartet sein. Gehen Sie dazu wie im *One Identity Manager Installationshandbuch* beschrieben vor.

Um einen Jobserver und seine Funktionen zu bearbeiten

1. Wählen Sie im Manager die Kategorie **IBM Notes | 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

- Stammdaten eines Jobservers auf Seite 80
- Festlegen der Serverfunktionen auf Seite 83

Verwandte Themen

- Installation und Konfiguration des One Identity Manager Service auf Seite 21

Stammdaten eines Jobservers

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 20: Eigenschaften eines Jobservers

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS Syntax. Beispiel: `<Name des Servers>.<Vollqualifizierter Domänenname>`

Eigenschaft	Bedeutung
Server ist Cluster	Angabe, 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. 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. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte

Eigenschaft	Bedeutung
	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 entsprechend einzutragen.
One Identity Manager Service installiert	Angabe, 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	Angabe, 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 Rechten im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*.
Kein automatisches Softwareupdate	Angabe, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.
Softwareupdate läuft	Angabe, ob gerade eine Softwareaktualisierung ausgeführt wird.
Letzter Abrufzeitpunkt	Zeitpunkt der letzten Prozessabholung.
Letzte Timeout Prüfung	Zeitpunkt der letzten Prüfung für geladene Prozessschritte, deren Auslieferung den Wert im Konfigurationsparameter **Common | Jobservice | LoadedJobsTimeOut** überschreitet.
Serverfunktion	Funktion des Servers in der One Identity Manager-Umgebung.

Eigenschaft	Bedeutung
	Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

Verwandte Themen

- Festlegen der Serverfunktionen auf Seite 83

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 21: Zulässige Serverfunktionen

Serverfunktion	Anmerkungen
CSV Konnektor	Server, auf dem der CSV Konnektor für die Synchronisation installiert ist.
Domänen-Controller	Active Directory Domänen-Controller. Server, die nicht als Domänen-Controller gekennzeichnet sind, werden als Memberserver betrachtet.
Druckserver	Server, der als Druckserver arbeitet.
Generischer Server	Server für die generische Synchronisation mit einem kundendefinierten Zielsystem.
Homeserver	Server zur Anlage von Homeverzeichnissen für Benutzerkonten.
IBM Notes Gateway Server	Gateway Server für die Synchronisation des One Identity Manager mit der IBM Notes-Umgebung.
IBM Notes Konnektor	Server, auf dem der IBM Notes Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem IBM Notes aus.
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.

Serverfunktion	Anmerkungen
	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.
Nativer Datenbankkonnektor	Der Server kann sich mit einer ADO.Net Datenbank verbinden.
One Identity Manager-Datenbankkonnektor	Server, auf dem der One Identity Manager Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem One Identity Manager aus.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
Primärer Domänen-Controller	Primärer Domänen-Controller.
Profilserver	Server für die Einrichtung von Profilverzeichnissen für Benutzerkonten.
SAM Synchronisationsserver	Server für die Synchronisation mit einem SMB-basierten Zielsystem aus.
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 Berichtserver	Server, auf dem die Berichte generiert werden.
Windows PowerShell Konnektor	Der Server kann Windows PowerShell Version 3.0 oder neuer ausführen.

Verwandte Themen

- Stammdaten eines Jobservers auf Seite 80

Zielsystemverantwortliche

Im One Identity Manager ist eine Standardanwendungsrolle für die Zielsystemverantwortlichen vorhanden. Weisen Sie dieser Anwendungsrolle die Personen zu, die berechtigt sind, alle Domänen im One Identity Manager zu bearbeiten.

Wenn Sie die Bearbeitungsrechte der Zielsystemverantwortlichen auf einzelne Domänen 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 Domänen 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 Domänen zuweisen.

Tabelle 22: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | IBM Notes** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen. • 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.

Benutzer	Aufgaben
	• Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

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 | IBM Notes**.
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 **IBM Notes | 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 Domänen festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **IBM Notes | Domänen**.
3. Wählen Sie in der Ergebnisliste die Domäne.
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 | IBM Notes** 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, die Domäne im One Identity Manager zu bearbeiten.

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer IBM Notes-Umgebung auf Seite 12
- Allgemeine Stammdaten einer Notes Domäne auf Seite 88

4

Notes Domänen

Im One Identity Manager entspricht eine Domäne der Abbildung eines Sichtbarkeitsbereiches im IBM Notes, beispielsweise einer produktiven IBM Notes-Umgebung. Durch dieses Konstrukt, das im One Identity Manager wesentlich stringenter behandelt wird als im IBM Notes, ist es möglich, mehrere produktive IBM Notes-Umgebungen parallel mit einer One Identity Manager-Datenbank zu verwalten. Auch wenn im IBM Notes die Beziehung eines Benutzers zu seiner Domäne nicht gepflegt ist, ist der One Identity Manager in der Lage, die aktuelle Domäne jedem Benutzerkonto zuzuordnen und somit die Umgebungen zu trennen.

HINWEIS: Die Einrichtung der Domänen in der One Identity Manager-Datenbank übernimmt der Synchronization Editor.

Um die Stammdaten einer Domäne zu bearbeiten

1. Wählen Sie die Kategorie **IBM Notes | Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für eine Domäne.
5. Speichern Sie die Änderungen.

Allgemeine Stammdaten einer Notes Domäne

Auf dem Tabreiter **Allgemein** erfassen Sie folgende Stammdaten.

Tabelle 23: Allgemeine Stammdaten einer Notes Domäne

Eigenschaft	Beschreibung
Vollständiger Name	Vollständiger Name der Domäne.
Anzeigename	Anzeigename zur Anzeige der Domäne in der Benut-

Eigenschaft	Beschreibung
	zeroberfläche.
Kontendefinition (initial)	Initiale Kontendefinition zur Erzeugung von Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für diese Domäne 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 Domäne festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte der Domäne, der sie zugeordnet sind. Jeder Domäne können andere Zielsystemverantwortliche zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle, deren Mitglieder verantwortlich für die Administration dieser Domäne sind. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.
Synchronisiert durch	Art der Synchronisation, über welche die Daten zwischen der Domäne und dem One Identity Manager ausgetauscht werden. Sobald Objekte für diese Domäne im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden. Beim Erstellen einer Domäne mit dem Synchronization Editor wird **One Identity Manager** verwendet.

Tabelle 24: Zulässige Werte

Wert	Synchronisation durch	Provisionierung durch
One Identity Manager	IBM Notes Konnektor	IBM Notes Konnektor
Keine Synchronisation	keine	keine

HINWEIS: Wenn Sie **Keine Synchronisation** festlegen, definieren Sie unternehmensspezifische Prozesse, um

Eigenschaft	Beschreibung
	Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.
Pfad der Benutzer-ID-Dateien	Pfad auf dem Gateway Server, der zur Erstellung neuer Benutzer-ID-Dateien genutzt wird. Diese Angabe wird nur benötigt, wenn der Konfigurationsparameter **TargetSystem | NDO | StoreIDInAddressbook** deaktiviert ist.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
ID-Vault aktiv	Angabe, ob zum Wiederherstellen der Benutzer-ID-Dateien die ID-Vault-Funktion von IBM Notes genutzt wird.

Verwandte Themen

- Einrichten von Kontendefinitionen auf Seite 47
- Zuweisen der Kontendefinition an ein Zielsystem auf Seite 62
- Zielsystemverantwortliche auf Seite 85
- Wiederherstellen der Benutzer-ID-Dateien auf Seite 137

Festlegen der Kategorien für die Vererbung von Notes Gruppen

Im One Identity Manager können Gruppen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen 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. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 31**.

Um Kategorien zu definieren

1. Wählen Sie im Manager in der Kategorie **IBM Notes | Domäne** die Domäne.
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 Notes Gruppen anhand von Kategorien auf Seite 158

Synchronisationsprojekt bearbeiten

Synchronisationsprojekte, in denen eine Domäne 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 die Kategorie **IBM Notes | Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten...**.

Verwandte Themen

- Anpassen einer Synchronisationskonfiguration auf Seite 33

5

Notes Zertifikate

Zertifikate werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen, damit sie bei der Anlage neuer Benutzerkonten referenziert werden können. Benutzerkonten, die mit dem One Identity Manager angelegt wurden, enthalten einen Verweis auf das verwendete Zertifikat. Dadurch können deren ID-Dateien jederzeit mit diesem Zertifikat wiederhergestellt werden. Bei der Verwaltung der Benutzerkonten über Kontendefinitionen ist das Zertifikat ausschlaggebend für die Bildung der weiteren Eigenschaften des Benutzerkontos.

Es können nur Zertifikate aus dem Domino-Verzeichnis synchronisiert werden. Wurde ein Benutzer im Zielsystem mit einem externen Zertifikat erstellt, kann der One Identity Manager das Zertifikat nicht ermitteln und damit nicht dem Benutzerkonto zuordnen.

Um ein Zertifikat zu bearbeiten

1. Wählen Sie die Kategorie **IBM Notes | Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Notes Zertifikate auf Seite 92

Allgemeine Stammdaten für Notes Zertifikate

Auf dem Tabreiter **Allgemein** erfassen Sie folgende Stammdaten.

Tabelle 25: Allgemeine Stammdaten eines Notes Zertifikats

Eigenschaft	Beschreibung
Vollständiger Name	Vollständiger Name des Zertifizierers.
Übergeordnete Zulassungsstelle	Eindeutige Kennung des übergeordneten Zertifizierers. Anzugeben ist der Name des Ausstellers des Zertifikates.
Notes Domäne	Eindeutige Kennung der Domäne.
Notes Server	Notes Server, auf dem die Postfachdatei des Zertifizierers abgelegt ist.
Postfachdatei	Pfad zur Postfachdatei des Zertifizierers.
Name der ID-Datei (inkl. Pfad)	Name und Pfad zur ID-Datei des Zertifizierers. Wenn mit dem Zertifikat Benutzerkonten registriert werden sollen, geben Sie den kompletten Dateipfad zur ID-Datei des Zertifizierers an. Das Verzeichnis, in dem die ID-Datei gespeichert ist, muss vom Gateway Server aus erreichbar sein. Diese Angabe wird nur benötigt, wenn die Option **CA-Prozess möglich** deaktiviert ist.
Kennwort und Kennwortbestätigung	Kennwort für die ID-Datei des Zertifizierers. Diese Angabe wird nur benötigt, wenn die Option **CA-Prozess möglich** deaktiviert ist.
CA-Prozess möglich	Angabe, ob für die Zertifizierung von Benutzerkonten der CA-Prozess genutzt werden soll. Wenn die Option deaktiviert ist, wird eine Zertifizierer-ID-Datei benötigt, um Benutzerkonten zu zertifizieren.
CA-Datenbankserver	Server, der die CA-Datenbank für dieses Zertifikat vorhält. Diese Angabe wird nur benötigt, wenn die Option **CA-Prozess möglich** aktiviert ist.
Name der CA-Datenbank	Name oder Pfad der CA-Datenbankdatei. Diese Angabe wird nur benötigt, wenn die Option **CA-Prozess möglich** aktiviert ist.
Ablaufdatum	Ablaufdatum des Zertifikats.
Zertifikatstyp	Typ des Zertifikats.

Kontaktdaten von Notes Zertifikaten

Auf dem Tabreiter **Kontakt** erfassen Sie die Kontaktdaten eines Zertifizierers.

Tabelle 26: Kontaktdaten eines Notes Zertifizierers

Eigenschaft	Beschreibung
Firma	Firma des Zertifizierers.
Abteilung	Abteilung des Zertifizierers.
Standort	Standort des Zertifizierers.
E-Mail-Adresse	E-Mail-Adresse des Zertifizierers.
Telefon Büro	Telefonnummer des Zertifizierers.
Kommentar	Freitextfeld für zusätzliche Erläuterungen.

Zusätzliche Aufgaben zur Verwaltung von Notes Zertifikaten

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

Überblick über das Notes Zertifikat

Um einen Überblick über ein Zertifikat zu erhalten

1. Wählen Sie die Kategorie **IBM Notes | Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat.
3. Wählen Sie die Aufgabe **Überblick über das Notes Zertifikat**.

Eigentümer zuweisen

Legen Sie fest, welche Benutzerkonten und Gruppen als Eigentümer des Zertifikatsdokuments eingetragen werden.

Um Benutzerkonten als Eigentümer für ein Zertifikat festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".

5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Eigentümer für ein Zertifikat festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Administratoren zuweisen

Legen Sie fest, welche Benutzerkonten und Gruppen das Zertifikatsdokument administrieren dürfen.

Um Benutzerkonten als Administratoren für ein Zertifikat festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat.
3. Wählen Sie die Aufgabe **Administratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Administratoren für ein Zertifikat festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat.
3. Wählen Sie die Aufgabe **Administratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".

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

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Nachbehandlung neu eingelesener Zertifikate

Um über den One Identity Manager neue Benutzerkonten anlegen oder vorhandene Benutzerkonten rezertifizieren zu können, übernehmen Sie neue Zertifikate regelmäßig in das persönliche Adressbuch des Synchronisationsbenutzers.

Um neue Zertifikate für die Registrierung von Benutzerkonten nutzen zu können

1. Übernehmen Sie die Zertifikate aus dem Domino-Verzeichnis in das persönliche Adressbuch des Synchronisationsbenutzers.

   Weitere Informationen finden Sie unter Übernehmen der Notes Zertifikate auf Seite 20.
2. Prüfen Sie, ob die Zertifikat-ID-Dateien vom Gateway Server aus erreichbar sind.
3. Tragen Sie Namen und Pfad der Zertifikat-ID-Dateien auf dem Gateway Server in die Stammdaten der Zertifikate im One Identity Manager ein. Diese Angabe wird nur für Zertifikate benötigt, die nicht mit dem CA-Prozess genutzt werden.

   Weitere Informationen finden Sie unter Allgemeine Stammdaten für Notes Zertifikate auf Seite 92.

Notes Zertifikatsanforderungen

Zertifikatsanforderungen werden für alle Dokumente, die über den CA-Prozess zertifiziert wurden, in der One Identity Manager-Datenbank abgebildet. Alle Zertifikatsanforderungen eines Zertifikats werden auf dem Überblicksformular des Zertifikats angezeigt.

Um die Eigenschaften einer Zertifikatsanforderung anzuzeigen

1. Wählen Sie die Kategorie **IBM Notes | Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat. Wählen Sie die Aufgabe **Überblick über das Notes Zertifikat**.
3. Wählen Sie auf dem Formularelement **Notes Zertifikatsanforderungen** eine Zertifikatsanforderung.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Tabelle 27: Stammdaten einer Notes Zertifikatsanforderung

Eigenschaft	Beschreibung
Objekt	Name des zertifizierten Objekts.
CA-Zertifikat	Name des Zertifikats, das für die Zertifizierung genutzt wurde.
Bearbeiter	Name des zulassenden Zertifizierers.
Zertifikat	Eindeutige Kennung des Zertifikats.
Notes Domäne	Domäne der Zertifikatsanforderung.
Anforderungsstatus	Verarbeitungsstatus der Zertifikatsanforderung.

6

Notes Schablonen

Damit der IBM Notes Konnektor im Zielsystem Benutzer anlegen kann, muss an den Benutzerkonten angegeben sein, welche Schablone beim Erzeugen der Postfachdatei für den Benutzer verwendet werden soll. Zu diesem Zweck werden im One Identity Manager Notes Schablonen abgebildet.

Um die Stammdaten einer Schablone zu bearbeiten

1. Wählen Sie die Kategorie **IBM Notes | Notes Schablonen**.
2. Wählen Sie in der Ergebnisliste die Schablone. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Tabelle 28: Stammdaten einer Notes Schablone

Eigenschaft	Beschreibung
Notes Schablone	Name der Schablone.
Notes Domäne	Domäne, in welcher die Schablone angewendet wird.
Dateiname	Name der Schablonendatei.

7

Notes Richtlinien

Über Richtlinien werden Einstellungen festgelegt, die auf Notes Benutzer und Gruppen angewendet werden. Richtlinien und Richtlinieneinstellungen können durch die Synchronisation in die One Identity Manager-Datenbank eingelesen und an Benutzerkonten zugeordnet werden. Den Richtlinien können Benutzerkonten und Gruppen als Mitglieder, Eigentümer oder Administratoren zugewiesen werden.

Um die Stammdaten von Richtlinien anzuzeigen

1. Wählen Sie die Kategorie **IBM Notes | Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Richtlinie. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Tabelle 29: Stammdaten einer Notes Richtlinie

Eigenschaft	Beschreibung
Bezeichnung	Name der Richlinie.
Vollständiger Name	Vollständiger Name der Richtlinie.
Übergeordnete Richtlinie	Übergeordnete Richtlinie.
Beschreibung	Beschreibung der Richtlinie.
Typ der Richtlinie	Typ der Richtlinie.
Kategorie	Kategorie der Richtlinie.
Ausnahmerichtlinie	Angabe, ob die Richtlinieneinstellungen anderer Richtlinien ignoriert werden sollen.
Archivierungsrichtlinie	Zugeordnete Archivierungsrichtlinieneinstellung.
Desktoprichtlinie	Zugeordnete Desktoprichtlinieneinstellung.
Mailrichtlinie	Zugeordnete Mailrichtlinieneinstellung.
Registrierungsrichtlinie	Zugeordnete Registrierungsrichtlinieneinstellung.
Sicherheitsrichtlinie	Zugeordnete Sicherheitsrichtlinieneinstellung.
Konfigurationsrichtlinie	Zugeordnete Konfigurationsrichtlinieneinstellung.

Verwandte Themen

- Notes Richtlinieneinstellungen auf Seite 102

Zusätzliche Aufgaben zur Verwaltung von Notes Richtlinien

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

Überblick über die Notes Richtlinie

Um einen Überblick über eine Richtlinie zu erhalten

1. Wählen Sie die Kategorie **IBM Notes | Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Richtlinie.
3. Wählen Sie die Aufgabe **Überblick über die Notes Richtlinie**.

Mitglieder an eine Notes Richtlinie zuweisen

Weisen Sie die Benutzerkonten und Gruppen zu, auf die die Richtlinie angewendet werden soll.

Um Benutzerkonten an eine Richtlinie zuzuweisen

1. Wählen Sie die Kategorie **IBM Notes | Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat.
3. Wählen Sie die Aufgabe **Mitglieder zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen an eine Richtlinie zuzuweisen

1. Wählen Sie die Kategorie **IBM Notes | Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat.

3. Wählen Sie die Aufgabe **Mitglieder zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Eigentümer an eine Notes Richtlinie zuweisen

Für Richtlinien können Sie Eigentümerbeziehungen definieren. Dafür legen Sie fest, welche Benutzerkonten und Gruppen die Richtlinie bearbeiten dürfen.

Um Benutzerkonten als Eigentümer zuzuweisen

1. Wählen Sie die Kategorie **IBM Notes | Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Eigentümer zuzuweisen

1. Wählen Sie die Kategorie **IBM Notes | Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Administratoren an eine Notes Richtlinie zuweisen

Für Richtlinien können Sie Administratorenbeziehungen definieren. Dafür legen Sie fest, welche Benutzerkonten und Gruppen die Richtlinie administrieren dürfen.

Um Benutzerkonten als Administratoren zuzuweisen

1. Wählen Sie die Kategorie **IBM Notes | Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat.
3. Wählen Sie die Aufgabe **Administratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Administratoren zuzuweisen

1. Wählen Sie die Kategorie **IBM Notes | Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat.
3. Wählen Sie die Aufgabe **Administratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Notes Richtlinieneinstellungen

Im One Identity Manager werden die Richtlinieneinstellungen abgebildet, die in den synchronisierten Notes Richtlinien genutzt werden.

Um die Stammdaten von Richtlinieneinstellungen anzuzeigen

1. Wählen Sie die Kategorie **IBM Notes | Richtlinien**.
2. Wählen Sie in der Ergebnisliste eine Richtlinie. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

3. Wählen Sie eine zugeordnete Richtlinieneinstellung und öffnen Sie das Kontextmenü dieser Zuordnung.
4. Klicken Sie **Gehe zum zugewiesenen Objekt**.
5. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Tabelle 30: Stammdaten einer Notes Richtlinieneinstellung

Eigenschaft	Beschreibung
Vollständiger Name	Vollständiger Name der Richtlinieneinstellung.
Beschreibung	Beschreibung der Richtlinieneinstellung.
Einstellungstyp	Typ der Richtlinieneinstellung.
Notes Domäne	Domäne der Richtlinieneinstellung.

Verwandte Themen

- Notes Richtlinien auf Seite 99

8

Notes Benutzerkonten

Mit dem One Identity Manager verwalten Sie die Benutzer und Personendokumente einer IBM Notes-Umgebung. Diese werden in der One Identity Manager-Datenbank als Notes Benutzerkonten abgebildet. Es werden alle Benutzerkonten abgebildet, die im Domino-Verzeichnis bekannt sind. Über die Mitgliedschaft in Gruppen und über die zugewiesenen Richtlinien erhalten die Benutzer Zugriff auf die Netzwerkressourcen.

Beim Anlegen eines Benutzers werden die Benutzer-ID-Datei zur Authentifizierung, die Postfachdatei sowie das persönliche Adressbuch des Benutzers erzeugt. Die Postfachdatei wird auf dem angegebenen Mailserver erzeugt, die ID-Datei und das persönliche Adressbuch entstehen auf dem Gateway-Server.

Wenn beim Einfügen eines neuen Benutzerkontos im One Identity Manager kein Zertifikat zugeordnet wird, wird im Zielsystem nur das Personendokument erstellt. Es werden keine Benutzer-ID-Datei, keine Postfachdatei und kein persönliches Adressbuch erzeugt.

Detaillierte Informationen zum Thema

- Benutzerkonten mit Personen verbinden auf Seite 104
- Unterstützte Typen von Benutzerkonten auf Seite 105
- Erfassen der Stammdaten für Notes Benutzerkonten auf Seite 110

Benutzerkonten mit Personen verbinden

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 Notes Domäne, wird durch die Zuweisung der Kontendefinition an eine Person über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

  Auch Personendokumente können über Kontendefinitionen erstellt werden.

  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.

Verwandte Themen

- Erfassen der Stammdaten für Notes Benutzerkonten auf Seite 110
- Einrichten von Kontendefinitionen auf Seite 47
- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 129
- Ausführliche Informationen zu den Grundlagen zur Behandlung und Administration von Personen und Benutzerkonten finden Sie im One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

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 31: 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 beispielsweise zu Trainingszwecken genutzt wird.	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 organisatorische 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 Dummy-Personen, die keinen Bezug zu einer realen Person haben. Diese Dummy-Personen werden benötigt, um Berechtigungen an die Benutzerkonten vererben zu können. Bei der Auswertung von Berichten,

Attestierungen oder Complianceprüfungen prüfen Sie, ob die Dummy-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.

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.

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**.

Administrative Benutzerkonten können Sie als **Persönliche Administratoridentität** oder als **Gruppenidentität** kennzeichnen. Um die Personen, welche diese Benutzerkonten nutzen, mit den benötigten Berechtigungen zu versorgen, gehen Sie folgendermaßen vor.

- Persönliche Administratoridentität
  1. Verbinden Sie das Benutzerkonto über die Spalte `UID_Person` mit einer Person.

     Nutzen Sie eine Person mit derselben Identität oder erstellen Sie eine neue Person.
  2. Weisen Sie diese Person an hierarchische Rollen zu.
- Gruppenidentität
  1. Weisen Sie dem Benutzerkonto alle Personen mit Nutzungsberechtigungen zu.
  2. Verbinden Sie das Benutzerkonto über die Spalte `UID_Person` mit einer Dummy-Person.

     Nutzen Sie eine Person mit derselben Identität oder erstellen Sie eine neue Person.
  3. Weisen Sie diese Dummy-Person an hierarchische Rollen zu.

  Das Benutzerkonto erhält seine Berechtigungen über die Dummy-Person.

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.

Erfassen der Stammdaten für Notes Benutzerkonten

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.

Um ein Benutzerkonto zu erstellen

1. Wählen Sie im Manager die Kategorie **IBM Notes | Benutzerkonten**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

Um die Stammdaten eines Benutzerkontos zu bearbeiten

1. Wählen Sie im Manager die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

Um ein Benutzerkonto für eine Person manuell zuzuweisen oder zu erstellen

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines Notes Benutzerkontos auf Seite 111
- Zusätzliche Stammdaten eines Notes Benutzerkontos auf Seite 118
- E-Mail-System eines Notes Benutzerkontos auf Seite 115
- Adressangaben eines Notes Benutzerkontos auf Seite 117
- Administrative Daten eines Notes Benutzerkontos auf Seite 119

Verwandte Themen

- Einrichten von Kontendefinitionen auf Seite 47
- Unterstützte Typen von Benutzerkonten auf Seite 105
- Benutzerkonten mit Personen verbinden auf Seite 104

Allgemeine Stammdaten eines Notes Benutzerkontos

Tabelle 32: Konfigurationsparameter für die Risikobewertung von Benutzerkonten

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

Auf dem Tabreiter **Allgemein** erfassen Sie folgende Stammdaten.

Tabelle 33: Allgemeine Stammdaten eines Notes Benutzerkontos

Eigenschaft	Beschreibung
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

Eigenschaft	Beschreibung
	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.
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. Auch Personendokumente können über Kontendefinitionen erstellt werden.
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.
Vorname	Vorname des Benutzers.
Zweiter Vorname	Zweiter Vorname des Benutzers.
Nachname	Nachname des Benutzers.
Kurzname	Kurzname des Benutzers.
Phonetischer Name	Name des Benutzers in phonetischer Schreibweise.
Notes Domäne	Domäne des Benutzerkontos.
Zertifikat	Zertifikat, mit dem die Benutzer-ID-Datei und die Postfachdatei des Benutzers registriert werden sollen (bei Neuanlage) oder registriert wurden. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. Reinen Personendokumenten ist kein Zertifikat zugeordnet. Wenn beim Speichern eines neuen Benutzerkontos kein Zertifikat zugeordnet ist, kann auch nachträglich kein Zertifikat zugeordnet werden.

Eigenschaft	Beschreibung
	Wenn beim Speichern eines neuen Benutzerkontos ein Zertifikat zugeordnet ist, kann das Zertifikat nicht nachträglich entfernt werden.
Organisatorische Einheit	Zusätzliche organisatorische Einheit, der das Benutzerkonto angehört.
Anzeigename	Anzeigename des Benutzerkontos. Der Anzeigename wird aus dem vollständigen Namen oder dem Vor- und Nachnamen gebildet.
Titel	Titel des Benutzers.
Generationskennzeichen	Generationskennzeichen des Benutzers, beispielsweise "Junior".
Alternative Sprache	Sprache des alternativen Namens.
Alternativer Name	Alternativer Name in der Muttersprache des Benutzers. Kann zur Anzeige und Namenssuche in der IBM Notes-Umgebung verwendet werden. Der alternative Name muss mit einer alternativen Sprache des Benutzerkontos verbunden sein.
E-Mail-System	Typ des E-Mail-Systems, welches das Benutzerkonto verwendet. Standardmäßig wird "1 - Notes" eingetragen. Abhängig vom gewählten E-Mail-System werden weitere Eingabefelder auf dem Stammdatenformular angezeigt.
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 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.
Benutzerkonto ist deaktiviert	Angabe, ob das Benutzerkonto für die Anmeldung an der Domäne gesperrt ist.
Identität	Typ der Identität des Benutzerkontos. Zulässige Werte sind: • **Primäre Identität**: Standardbenutzerkonto einer Person. • **Organisatorische Identität**: Sekundäres

Eigenschaft	Beschreibung
	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 beispielsweise zu Trainingszwecken genutzt wird. • **Gruppenidentität**: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird. Weisen Sie alle Personen zu, die das Benutzerkonto nutzen. • **Dienstidentität**: Dienstkonto.
Privilegiertes Benutzerkonto	Angabe, ob es sich um ein privilegiertes Benutzerkonto handelt.
Gruppen erbbar	Angabe, ob das Benutzerkonto Gruppen über die Person erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen oder 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 der Person diese Gruppe nur, wenn die Option aktiviert ist.

Verwandte Themen

- Einrichten von Kontendefinitionen auf Seite 47
- Benutzerkonten mit Personen verbinden auf Seite 104
- Unterstützte Typen von Benutzerkonten auf Seite 105
- E-Mail-System eines Notes Benutzerkontos auf Seite 115
- Festlegen der Kategorien für die Vererbung von Notes Gruppen auf Seite 90
- Sperren und Entsperren von Notes Benutzerkonten auf Seite 140

E-Mail-System eines Notes Benutzerkontos

Tabelle 34: Konfigurationsparameter für die Erzeugung der Postfachdateien

Konfigurationsparameter	Wirkung bei Aktivierung
TargetSystem\NDO\CreateMailDB	Der Konfigurationsparameter legt fest, ob die Postfachdatei nach oder während der Registrierung des Notes Benutzers im Zielsystem erzeugt wird. Wenn der Konfigurationsparameter aktiviert ist, wird die Postfachdatei während der Registrierung erzeugt. Dabei wird die Schablone des Notes Servers verwendet, auf dem der Benutzer registriert wird. Wenn der Konfigurationsparameter deaktiviert ist (Standard), wird die Postfachdatei nach der Registrierung des Notes Benutzers erzeugt. Dabei wird die Schablone verwendet, die am Benutzerkonto oder im Konfigurationsparameter „TargetSystem\NDO\DefTemplatePath" angegeben ist.
TargetSystem\NDO\DefTemplatePath	Schablone zum Anlegen der Postfachdateien auf einem Notes Server.
TargetSystem\NDO\MailFilePath	Verzeichnis auf dem Mailserver, in dem die Postfachdateien der Benutzerkonten abgelegt werden.

Im Eingabefeld **E-Mail-System** unter den allgemeinen Stammdaten wählen Sie das E-Mail-System aus, welches das Benutzerkonto verwendet. Zur Auswahl stehen:

- 1 - Notes
- 2 - cc:Mail
- 3 - Other
- 4 - X.400
- 5 - Other Internet Mail
- 6 - POP or IMAP
- 100 - None

  Wird kein Mailsystem genutzt, geben Sie den Typ „None" an.

Abhängig vom gewählten E-Mail-System werden die nachfolgend beschriebenen Eigenschaften zur Adressierung eingeblendet.

HINWEIS: Prüfen Sie, ob für das gewählte E-Mail-System der Mailserver und der Name der Postfachdatei benötigt werden. Damit die Postfachdatei erzeugt werden kann, erfassen Sie die benötigten Daten.

Tabelle 35: E-Mail-System-Daten eines Notes Benutzerkontos

E-Mail-System	Eigenschaft	Beschreibung
Notes POP or IMAP	Mailserver	Notes Server, der als Mailserver genutzt wird. Es stehen alle Notes Server zur Auswahl, die mit der Option **Hat Notes Postfachdateien** gekennzeichnet sind.
Notes	Schablone für Postfachdatei	Name der Notes Schablone, die zum Erstellen der Postfachdatei genutzt wird. Die Schablone bestimmt, welche Clientversion zur Erzeugung der Postfachdatei für das Benutzerkonto verwendet wird. Die Schablone muss auf dem Gateway Server vorhanden sein. Die Ermittlung der Daten kann über die IT Betriebsdaten einer Person erfolgen. Ist keine Schablone angegeben, wird die im Konfigurationsparameter "TargetSystem\NDO\DefTemplatePath" hinterlegte Schablone verwendet.
Notes POP or IMAP	Postfachdatei	Pfadangabe und Name der Postfachdatei. Diese werden per Bildungsregel gebildet. Die Postfachdatei wird auf dem angegebenen Mailserver in einem gesonderten Verzeichnis unterhalb des Installationsverzeichnisses abgelegt. Der Verzeichnisname ist im Konfigurationsparameter "TargetSystem\NDO\MailFilePath" hinterlegt. Um ein anderes Verzeichnis zu verwenden, bearbeiten Sie im Designer den Wert des Konfigurationsparameters.
Notes POP or IMAP	Anzeigename der Postfachdatei	Anzeigename der Postfachdatei. Er wird per Bildungsregel aus dem Vor- und Nachnamen und dem Zusatz "Mailfile" gebildet.
Notes Other Other Internet Mail POP or IMAP	Weiterleitungsadresse	E-Mail-Adresse, an die eingehende Nachrichten weitergeleitet werden. Es muss die vollständige E-Mail-Adresse (inklusive Domänenname) angegeben werden.
Notes	Nachrichtenspeicherung	Sichtbarkeitsbereich des Postfachspeichers. Zur

E-Mail-System	Eigenschaft	Beschreibung
POP or IMAP		Auswahl stehen: • 0 - Notes • 1 - Notes and Internet Mail • 2 - Internet Mail
Notes cc:Mail Other Other Internet Mail POP or IMAP	Internetadresse	Vollständige SMTP-Adresse des Benutzerkontos. Die Internetadresse dient zur Identifizierung des Nachrichtenempfängers, wenn in der IBM Notes-Umgebung Nachrichten über SMTP empfangen werden. Abhängig vom Automatisierungsgrad des Benutzerkontos wird die Internetadresse aus der Standard-E-Mail-Adresse der Person gebildet.
cc:Mail	cc:Mail Post Office	Post Office, in dem sich die Mailbox des Benutzers befindet.
cc:Mail	cc:Mail Benutzername	Benutzername der Mailbox.
cc:Mail	cc:Mail Standorttyp	Standorttyp der Mailbox. Wählen Sie „LOCAL" oder „REMOTE".
X.400	X.400 Server	Notes Server, der als X.400 Server genutzt wird. Es stehen alle Notes Server zur Auswahl, die mit der Option **Hat Notes Postfachdateien** gekennzeichnet sind.
X.400	X.400 Adresse	Mailadresse des Benutzers im X.400-Format (inklusive Domänenname).

Detaillierte Informationen zum Thema

- Erzeugen der Postfachdateien auf Seite 135

Adressangaben eines Notes Benutzerkontos

Auf den Tabreitern **Firma** und **Privat** erfassen Sie die Adressinformationen und die telefonischen Angaben zur Erreichbarkeit der Person, die dieses Benutzerkonto verwendet. Geben Sie weitere bekannte Angaben zur näheren Beschreibung dieser Person an. Abhängig vom Automatisierungsgrad des Benutzerkontos werden diese Angaben aus den Stammdaten der Person übernommen.

Zusätzliche Stammdaten eines Notes Benutzerkontos

Auf dem Tabreiter **Verschiedenes** erfassen Sie zusätzliche Angaben für ein Benutzerkonto, die hauptsächlich die Postfachdatei und die Übermittlung von Nachrichten betreffen. Die Größe der Postfachdatei eines Benutzerkontos kann regelmäßig über einen zeitgesteuerten Prozessauftrag ermittelt werden. Voraussetzung dafür ist die korrekte Angabe des Mailservers und des Pfads zur Postfachdatei auf dem Tabreiter **Allgemein**.

Um die Größe der Postfachdateien der Benutzerkonten zu ermitteln

- Konfigurieren und aktivieren Sie im Designer den Zeitplan **IBM Notes Größe der Postfachdateien einlesen**.

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

Tabelle 36: Zusätzliche Stammdaten eines Notes Benutzerkontos

Eigenschaft	Beschreibung
Größe [KB]	Logische Größe der Postfachdatei.
Physische Größe [KB]	Physische Größe der Postfachdatei.
Max. Größe [KB]	Maximal zulässige Größe der Postfachdatei.
Warnen ab [KB]	Schwellwert, bei dessen Überschreitung eine E-Mail an den Benutzer gesendet werden kann.
Internetkennwort/Kennwortbestätigung	Internetkennwort des Benutzers. Dieses Kennwort müssen Web-Benutzer verwenden, um sich an einem Domino-Web-Server zu authentifizieren. 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.
Sametime Server	Notes Server, der als Sametime Server genutzt wird. Für Benutzerkonten, welche die Sametime-Funktion von IBM Notes nutzen, geben Sie den Sametime Server an.
Kalenderdomäne	Domäne, die gilt, wenn das Benutzerkonto eine andere Kalender- und Zeitplanungsfunktion verwendet.
Webseite	Webseite des Benutzers.
Kommentar	Freitextfeld für zusätzliche Erläuterungen.

Verwandte Themen

- Kennwortrichtlinien für Notes Benutzerkonten auf Seite 65

Administrative Daten eines Notes Benutzerkontos

Auf dem Tabreiter **Administration** erfassen Sie die administrativen Daten eines Benutzerkontos.

Tabelle 37: Administrative Daten eines Notes Benutzerkontos

Eigenschaft	Beschreibung
Zugewiesene Richtlinie	Richtlinie, die explizit zugewiesen ist. Sie können eine Richtlinie zuweisen, die zur selben Domäne gehört, wie das Benutzerkonto. HINWEIS: Richtlinieneinstellungen ersetzen grundsätzlich alle Einstellungen am Benutzerkonto.
Kennwortprüftyp	Gibt an, wie sich ein Benutzer am Server authentifizieren muss. Die Kennwortprüftypen sind: **0 - don't check:** Kennwort nicht prüfen. Bei der Anmeldung am Server muss der Benutzer kein Kennwort eingeben. **1 - check:** Kennwort prüfen. Bei der Anmeldung am Server muss der Benutzer ein Kennwort eingeben. **2 - Lockout ID:** ID sperren. Der Benutzer kann sich an keinem Server in der Domäne anmelden, der Kennwörter prüft. Beim Anlegen eines neuen Benutzerkontos wird standardmäßig der Kennwortprüftyp **0 - don't check** übernommen.
Kennwortänderungsintervall	Kennwortänderungsintervall in Tagen. Nach Ablauf des Kennwortänderungsintervalls wird der Serverzugriff für den Benutzer gesperrt, bis dieser das Kennwort geändert hat.
Nachfrist	Nachfrist für die Kennwortänderung in Tagen. Wird das

Eigenschaft	Beschreibung
	Kennwort nicht innerhalb der angegebenen Nachfrist geändert, kann sich der Benutzer nicht mehr am Server anmelden.
Letztes Änderungsdatum	Datum der letzten Änderung des Benutzerkontos.
Letzte Änderung des Internetkennworts	Datum der letzten Änderung des Internetkennwortes.
Kennwort/Kennwortbestätigung	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 initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen. Für reine Personendokumente muss kein Kennwort angegeben werden. 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.
Kennwort bei der nächsten Anmeldung ändern	Angabe, ob das Kennwort des Benutzerkontos bei der nächsten Anmeldung am Zielsystem geändert werden muss.
Notes Client Lizenz	Lizenztyp des Notes Clients. Der Lizenztyp bestimmt den Umfang des Benutzerzugriffs. Die möglichen Lizenztypen sind: • 0 - IBM Notes • 1 - IBM Notes Mail • 2 - IBM Notes Desktop • 3 - IBM Notes Designer • 4 - IBM Notes Administration • 5 - IBM iNotes®/Domino® CAL Beim Anlegen eines neuen Benutzerkontos wird standardmäßig der Lizenztyp **0 - IBM Notes** übernommen.

Eigenschaft	Beschreibung
Setup Profil	Name des Benutzerkonfigurationsprofils, das bei der Einrichtung der Arbeitsumgebung verwendet wird.
Abgleich mit fremdem Verzeichnis erlaubt	Angabe, ob der Benutzername mit anderen Systemen synchronisiert werden kann.
Netzwerk-Benutzerkonto	Benutzerkonto, welches zur Synchronisation zwischen IBM Notes und anderen Systemen, beispielsweise Active Directory, verwendet wird.
Vollständiger Name	Vollständiger Name des Benutzerkontos. Der vollständige Name wird aus Vorname, Nachname, Zertifikat und organisatorischer Einheit gebildet.
ID läuft ab	Ablaufdatum der Benutzer-ID-Datei. Das Ablaufdatum wird über eine Bildungsregel berechnet. Benutzer-ID-Dateien für aktivierte Benutzerkonten, die in weniger als 10 Tagen ablaufen, können um 2 Jahre verlängert werden. ***Um das Ablaufdatum automatisch zu verlängern*** • Konfigurieren und aktivieren Sie im Designer den Zeitplan **IBM Notes ID-Ablaufdaten automatisch verlängern**. Ausführliche Informationen zum Konfigurieren von Zeitplänen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.

Verwandte Themen

- Notes Server auf Seite 177
- Kennwortrichtlinien für Notes Benutzerkonten auf Seite 65
- Initiales Kennwort für neue Notes Benutzerkonten auf Seite 76

Zusätzliche Aufgaben zur Verwaltung von Notes Benutzerkonten

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

Überblick über das Notes Benutzerkonto

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das Notes Benutzerkonto**.

Ändern des Automatisierungsgrades an einem Benutzerkonto

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 **IBM Notes | 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 eines Notes Benutzerkontos auf Seite 111

Notes Gruppen direkt an ein Notes Benutzerkonto zuweisen

Gruppen können einem Benutzerkonto direkt oder indirekt zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der Gruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person ein Notes Benutzerkonto, werden die Gruppen der hierarchischen Rollen an dieses Benutzerkonto vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Gruppen direkt zuweisen.

Um Gruppen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **IBM Notes | 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. Um die angezeigten Gruppen zu filtern, wählen Sie im Eingabefeld **Notes Domänen** eine Domäne aus.

   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.

Benutzerkonten können nicht direkt in dynamische Gruppen aufgenommen werden. Über Einschlusslisten können Benutzerkonten zusätzlich an dynamische Gruppen zugewiesen werden.

Verwandte Themen

- Notes Gruppen an Notes Benutzerkonten zuweisen auf Seite 147
- Ausschluss- und Einschlusslisten pflegen auf Seite 128
- Mitgliedschaften in dynamischen Gruppen auf Seite 167

Eigentümer für Dokumente festlegen

Legen Sie fest, für welche Dokumente das Benutzerkonto als Eigentümer eingetragen wird. Es können nur Dokumente zugewiesen werden, die zur selben Domäne gehören, wie das Benutzerkonto.

Um den Eigentümer für Benutzerkonten festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Dokumenteigentümer zuweisen**.
4. Wählen Sie den Tabreiter **Benutzer**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um den Eigentümer für Gruppen festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Dokumenteigentümer zuweisen**.
4. Wählen Sie den Tabreiter **Gruppe**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Um den Eigentümer für Mail-In-Datenbanken festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Dokumenteigentümer zuweisen**.
4. Wählen Sie den Tabreiter **Mail-In-DB**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Mail-In-Datenbanken zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Mail-In-Datenbanken.
6. Speichern Sie die Änderungen.

Um den Eigentümer für Zertifikate festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Dokumenteigentümer zuweisen**.
4. Wählen Sie den Tabreiter **Zertifikate**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zertifikate zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Zertifikate.
6. Speichern Sie die Änderungen.

Um den Eigentümer für Serverdokumente festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Dokumenteigentümer zuweisen**.
4. Wählen Sie den Tabreiter **Server Dokument**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Serverdokumente zu.

   - ODER -

Entfernen Sie im Bereich **Zuordnungen entfernen** die Serverdokumente.

6. Speichern Sie die Änderungen.

Eigentümer zuweisen

Legen Sie fest, welche Benutzerkonten und Gruppen das ausgewählte Benutzerkonto bearbeiten dürfen.

Um Benutzerkonten als Eigentümer festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Wählen Sie den Tabreiter **Benutzer**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Eigentümer festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Wählen Sie den Tabreiter **Gruppe**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Administrierbare Dokumente zuweisen

Legen Sie fest, welche Dokumente das Benutzerkonto administrieren darf. Es können nur Dokumente zugewiesen werden, die zur selben Domäne gehören, wie das Benutzerkonto.

Um den Administrator für Benutzerkonten festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Administrierbare Dokumente zuweisen**.

4. Wählen Sie den Tabreiter **Benutzer**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um den Administrator für Gruppen festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Administrierbare Dokumente zuweisen**.
4. Wählen Sie den Tabreiter **Gruppe**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Um den Administrator für Mail-In-Datenbanken festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Administrierbare Dokumente zuweisen**.
4. Wählen Sie den Tabreiter **Mail-In-DB**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Mail-In-Datenbanken zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Mail-In-Datenbanken.
6. Speichern Sie die Änderungen.

Um den Administrator für Zertifikate festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Administrierbare Dokumente zuweisen**.
4. Wählen Sie den Tabreiter **Zertifikate**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zertifikate zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Zertifikate.
6. Speichern Sie die Änderungen.

Um den Administrator für Server festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Administrierbare Dokumente zuweisen**.
4. Wählen Sie den Tabreiter **Server**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Server zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Server.
6. Speichern Sie die Änderungen.

Um den Administrator für Serverdokumente festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Administrierbare Dokumente zuweisen**.
4. Wählen Sie den Tabreiter **Server Dokument**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Serverdokumente zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Serverdokumente.
6. Speichern Sie die Änderungen.

Administratoren zuweisen

Legen Sie fest, welche Benutzerkonten und Gruppen das ausgewählte Benutzerkonto administrieren dürfen.

Um Benutzerkonten als Administratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Administratoren zuweisen**.
4. Wählen Sie den Tabreiter **Benutzer**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Administratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Administratoren zuweisen**.
4. Wählen Sie den Tabreiter **Gruppen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Ausschluss- und Einschlusslisten pflegen

Über diese Aufgabe nehmen Sie das Benutzerkonto in die Ausschlussliste und die Einschlussliste dynamischer Gruppen auf.

Um ein Benutzerkonto in die Einschlussliste dynamischer Gruppen aufzunehmen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Ausschluss- und Einschlusslisten pflegen**.
4. Wählen Sie den Tabreiter **Einschlussliste**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu, in deren Einschlussliste das Benutzerkonto Mitglied werden soll.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Um ein Benutzerkonto in die Ausschlussliste dynamischer Gruppen aufzunehmen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Ausschluss- und Einschlusslisten pflegen**.
4. Wählen Sie den Tabreiter **Ausschlussliste**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu, in deren Ausschlussliste das Benutzerkonto Mitglied werden soll.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Mitgliedschaften in dynamischen Gruppen auf Seite 167

Zusatzeigenschaften zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

1. Wählen Sie die Kategorie **IBM Notes | 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.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Zusatzeigenschaften.
5. Speichern Sie die Änderungen.

Ausführliche Informationen zur Einrichtung von Zusatzeigenschaften finden Sie im One Identity Manager Administrationshandbuch für das Identity Management Basismodul.

Automatische Zuordnung von Personen zu Benutzerkonten

Tabelle 38: Konfigurationsparameter für die Synchronisation einer Notes Domäne

Konfigurationsparameter	Bedeutung
TargetSystem\NDO\ PersonAutoFullsync	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem\NDO\ PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem\NDO\ PersonExcludeList	Der Konfigurationsparameter enthält eine Auflistung aller Benutzerkonten, für die keine automatische

Konfigurationsparameter	Bedeutung
	Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird.
TargetSystem\NDO\ PersonAutoDisabledAccounts	Der Konfigurationsparameter legt fest, ob an gesperrte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.

Beim Einfügen eines Benutzerkontos kann automatisch eine vorhandene Person zugeordnet und im Bedarfsfall 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.

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\NDO\PersonAutoFullsync“ und wählen Sie den gewünschte Modus.
- Wenn Personen außerhalb der Synchronisation zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter „TargetSystem\NDO\PersonAutoDefault“ und wählen Sie den gewünschten Modus.
- Legen Sie im Konfigurationsparameter "TargetSystem\NDO\PersonExcludeList" die Benutzerkonten fest, für die keine automatische Zuordnung zu Personen erfolgen soll.

  Beispiel:

  ```
  ADMINISTRATOR
  ```

- Legen Sie über den Konfigurationsparameter "TargetSystem\NDO\PersonAutoDisabledAccounts" fest, ob an gesperrte

Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.

- Weisen Sie der Domäne eine Kontendefinition zu. Stellen Sie sicher, dass der Automatisierungsgrad, der verwendet werden soll, als Standardautomatisierungsgrad eingetragen ist.
- Definieren Sie die Suchkriterien für die Personenzuordnung der Domäne.

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 Domäne 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.

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie der Domäne 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 **IBM Notes | Benutzerkonten | Verbunden aber nicht konfiguriert | <Domäne>**.
    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.

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

Verwandte Themen

- Erstellen einer Kontendefinition auf Seite 47
- Zuweisen der Kontendefinition an ein Zielsystem auf Seite 62
- Bearbeiten der Suchkriterien für die automatische Personenzuordnung auf Seite 132

Bearbeiten der Suchkriterien für die automatische Personenzuordnung

Die Kriterien für die Personenzuordnung werden an der Domäne definiert. Dabei 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 `NDODomain` geschrieben.

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: Bei der Zuordnung der Personen zu Benutzerkonten anhand der Suchkriterien erhalten die Benutzerkonten 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.

Für administrative Benutzerkonten wird empfohlen, die Zuordnung nicht anhand der Suchkriterien vorzunehmen. Ordnen Sie Personen zu administrativen Benutzerkonten über die Aufgabe **Stammdaten bearbeiten** am jeweiligen Benutzerkonto zu.

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.

Um die Kriterien für die Personenzuordnung für eine Notes Domäne zu definieren

1. Wählen Sie die Kategorie **IBM Notes | Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.
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 39: Standardsuchkriterien für Benutzerkonten

Anwenden auf	Spalte an Person	Spalte am Benutzerkonto
Notes Benutzerkonten	Vorname (FirstName) UND Nachname (LastName)	Vorname (FirstName) UND Nachname (LastName)
Aktive Notes Benutzerkonten	Vorname (FirstName) UND Nachname (LastName)	Vorname (FirstName) UND Nachname (LastName)

5. Speichern Sie die Änderungen.

Direkte Zuordnung von Personen an Benutzerkonten anhand einer Vorschlagsliste

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

Tabelle 40: 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.

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

Um die Suchkriterien auf die Benutzerkonten anzuwenden

- Klicken Sie **Neu laden**.

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

Um Personen direkt über die Vorschlagsliste zuzuordnen

1. Klicken Sie **Vorgeschlagene Zuordnungen**.
    a. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die vorgeschlagene Person zugeordnet werden soll. Eine Mehrfachauswahl ist möglich.
    b. Klicken Sie **Ausgewählte zuweisen.**
    c. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

       Den ausgewählten Benutzerkonten werden die per Suchkriterium ermittelten Personen zugeordnet.

    – ODER –
2. Klicken Sie **Ohne Personenzuordnung**.
    a. Klicken Sie **Person auswählen** für das Benutzerkonto, dem eine Person zugeordnet werden soll. Wählen Sie eine Person aus der Auswahlliste.
    b. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die ausgewählten Personen zugeordnet werden sollen. Eine Mehrfachauswahl ist möglich.
    c. Klicken Sie **Ausgewählte zuweisen**.
    d. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

       Den ausgewählten Benutzerkonten werden die Personen zugeordnet, die in der Spalte **Person** angezeigt werden.

Um Zuordnungen zu entfernen

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

       Von den ausgewählten Benutzerkonten werden die zugeordneten Personen entfernt.

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

Verwandte Themen

- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 129

Erzeugen der Postfachdateien

Tabelle 41: Konfigurationsparameter für die Erzeugung der Postfachdateien

Konfigurationsparameter	Wirkung bei Aktivierung
TargetSystem\NDO\CreateMailDB	Der Konfigurationsparameter legt fest, ob die Postfachdatei nach oder während der Registrierung des Notes Benutzers im Zielsystem erzeugt wird. Wenn der Konfigurationsparameter aktiviert ist, wird die Postfachdatei während der Registrierung erzeugt. Dabei wird die Schablone des Notes Servers verwendet, auf dem der Benutzer registriert wird. Wenn der Konfigurationsparameter deaktiviert ist (Standard), wird die Postfachdatei nach der Registrierung des Notes Benutzers erzeugt. Dabei wird die Schablone verwendet, die am Benutzerkonto oder im Konfigurationsparameter "TargetSystem\NDO\DefTemplatePath" angegeben ist.
TargetSystem\NDO\DefTemplatePath	Schablone zum Anlegen der Postfachdateien auf einem Notes Server.
TargetSystem\NDO\MailFilePath	Verzeichnis auf dem Mailserver, in dem die Postfachdateien der Benutzerkonten abgelegt werden.

Ob und auf welchem Weg im IBM Notes Postfachdateien erzeugt werden, ist abhängig von den Angaben am Benutzerkonto und von den Einstellungen der Konfigurationsparameter. Damit eine Postfachdatei erzeugt wird, muss am Benutzerkonto Pfad und Dateiname der Postfachdatei angegeben sein. Fehlt diese Angabe, wird keine Postfachdatei erzeugt.

Der Konfigurationsparameter "TargetSystem\NDO\CreateMailDB" ist deaktiviert (Standard)

Standardmäßig wird die Postfachdatei nach der Registrierung des Notes Benutzers im Zielsystem erzeugt. Dabei wird die Schablone verwendet, die am Benutzerkonto angegeben ist. Ist dort keine Schablone für die Postfachdatei angegeben, wird die Schablone verwendet, die im Konfigurationsparameter "TargetSystem\NDO\DefTemplatePath" hinterlegt ist. Die Schablone muss auf dem Gateway Server vorhanden sein.

Der Konfigurationsparameter "TargetSystem\NDO\CreateMailDB" ist aktiviert

Wenn es erforderlich ist, dass die Postfachdatei bereits während der Registrierung des Notes Benutzers erzeugt wird, aktivieren Sie den Konfigurationsparameter "TargetSystem\NDO\CreateMailDB". In diesem Fall wird die Schablone des Notes Servers verwendet, auf dem der Benutzer registriert wird.

HINWEIS: Auf die so erzeugten Postfachdateien hat der One Identity Manager Service keinen Zugriff. Verschiedene Aktionen, wie beispielsweise das Auslesen der Größe der Postfachdateien, sind dadurch nicht möglich.

Aktivieren Sie den Konfigurationsparameter nur, wenn verhindert werden soll, dass der IBM Notes Konnektor auf die erzeugten Postfachdateien zugreift.

Verwandte Themen

- E-Mail-System eines Notes Benutzerkontos auf Seite 115
- Zusätzliche Stammdaten eines Notes Benutzerkontos auf Seite 118

Speichern der Benutzer-ID-Dateien

Tabelle 42: Konfigurationsparameter für die Erzeugung der Postfachdateien

Konfigurationsparameter	Wirkung bei Aktivierung
TargetSystem\NDO\StoreIDInAddressbook	Der Konfigurationsparameter regelt die Behandlung der ID-Dateien für neue Benutzerkonten. Ist der Konfigurationsparameter aktiviert, wird die erstellte ID-Datei als Attachment an das Personendokument angehängt. Ist der Konfigurationsparameter deaktiviert, wird die erstellte ID-Datei auf dem Gateway Server abgelegt.

Der IBM Notes Konnektor benötigt eine Information, wo die ID-Dateien für neue Benutzerkonten in der IBM Notes-Umgebung gespeichert werden sollen. Benutzer-ID-Dateien können als Attachment an das Personendokument angehängt oder auf dem Gateway Server abgelegt werden. Das gewünschte Verhalten stellen Sie am Konfigurationsparameter "TargetSystem\NDO\StoreIDInAddressbook" ein. Wenn die Benutzer-ID-Dateien auf dem Gateway Server abgelegt werden sollen, geben Sie den Pfad an, unter dem die Dateien gespeichert werden sollen.

Standardmäßig nutzt der IBM Notes Konnektor den Pfad, der an der Domäne hinterlegt ist. Wenn dort kein Standardpfad angegeben ist, können Sie den Pfad an den Mailservern der Benutzerkonten hinterlegen.

HINWEIS: Wenn der Pfad weder an der Domäne noch am Mailserver angegeben ist, nutzt der IBM Notes Konnektor den Standardpfad, der an der Variablen `UserIDFilesDefaultPath`

im Synchronisationsprojekt hinterlegt ist. Passen Sie die Synchronisationskonfiguration an, wenn Sie den Wert der Variablen ändern möchten. Ausführliche Informationen zu Variablen und Variablensets finden Sie im One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation

Um den Speicherort der Benutzer-ID-Dateien auf dem Gateway Server festzulegen

1. Deaktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\NDO\StoreIDInAddressbook".
2. Bearbeiten Sie im Manager die Stammdaten der Domäne und geben Sie den Pfad der Benutzer-ID-Dateien an.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Notes Domäne auf Seite 88
- Allgemeine Stammdaten von Notes Servern auf Seite 177
- E-Mail-System eines Notes Benutzerkontos auf Seite 115

Wiederherstellen der Benutzer-ID-Dateien

Wenn ein Benutzer das Kennwort zu seinem Benutzerkonto vergessen beziehungsweise die Benutzer-ID-Datei selbst verloren hat, kann die Benutzer-ID-Datei wiederhergestellt werden. IBM Notes stellt dafür seit der IBM Domino Version 8.5 die ID-Vault-Funktion zur Verfügung.

Mit dem "ID-Restore" stellt der One Identity Manager ein eigenes Verfahren zur Wiederherstellung der Benutzer-ID-Dateien bereit. Dieses kann angewendet werden, wenn eine ältere IBM Domino Version eingesetzt wird oder ID-Vault nicht genutzt werden soll.

HINWEIS: Welches Verfahren zum Wiederherstellen der Benutzer-ID-Dateien genutzt werden soll, wird an der Domäne festgelegt. Diese Auswahl gilt für alle Benutzerkonten der Domäne!

ID-Vault

Die ID-Vault ist eine IBM Domino Datenbank, die Kopien der Benutzer-ID-Dateien speichert. Damit ist IBM Notes in der Lage Benutzer-ID-Dateien wiederherzustellen und Kennwörter für Benutzerkonten zurückzusetzen. Der One Identity Manager stellt einen Prozess bereit, der Kennwörter in der ID-Vault zurücksetzt.

Voraussetzungen

- Der Domino-Server, mit dem der Gateway Server kommuniziert, ist gleichzeitig der ID-Vault-Server.
- Auf dem Serverdokument sind Ausführungsrechte für Agenten für das Benutzerkonto für die Synchronisation gesetzt. Weitere Informationen finden Sie unter Beschränkte LotusScript/Java-Agenten ausführen auf Seite 197.
- Berechtigungen auf die ID-Vault-Datenbank für das Benutzerkonto für die Synchronisation sind gesetzt: Zugriffsfunktion "Manager" und Rolle "Auditor". Ausführliche Informationen entnehmen Sie der Dokumentation Ihrer IBM Notes-Umgebung.
- Berechtigung zum Wiederherstellen der Kennwörter für das administrative Benutzerkonto für die Synchronisation und für den ID-Vault-Server sind gesetzt. Ausführliche Informationen entnehmen Sie der Dokumentation Ihrer IBM Notes-Umgebung.

Um ID-Vault zu nutzen

1. Wählen Sie die Kategorie **IBM Notes | Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne, für die Sie ID-Vault nutzen möchten, und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Aktivieren Sie die Option **ID-Vault aktiv**.

   Diese Einstellung wirkt auf alle Benutzerkonten der Domäne.
4. Speichern Sie die Änderungen.

HINWEIS: Werden durch die ID-Vault-Richtlinie im IBM Notes einzelne Benutzerkonten vom ID-Vault ausgenommen, kann das Kennwort auch durch den One Identity Manager nicht zurückgesetzt werden.

Damit ein Zurücksetzen der Kennwörter für alle Benutzerkonten einer Domäne möglich ist, weisen Sie dem ID-Vault eine organisationsweite Richtlinie zu.

Beim Publizieren eines neuen Benutzerkontos in die IBM Notes-Umgebung speichert der One Identity Manager das initiale Kennwort in die One Identity Manager-Datenbank (`NDOUser.PasswordInitial`). Dieses initiale Kennwort wird genutzt, wenn das Kennwort eines Benutzerkontos zurückgesetzt werden soll. Für Benutzerkonten, die im One Identity Manager angelegt wurden, wird das initiale Kennwort automatisch gespeichert. Für alle anderen Benutzerkonten muss das initiale Kennwort durch einen kundenspezifischen Prozess in die One Identity Manager-Datenbank übertragen werden.

Um das Kennwort für ein Benutzerkonto zurückzusetzen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **ID-Restore**.

Die Aufgabe startet den Prozess `NDO_NDOUser_PWReset_from_Vault`. Durch den Prozess wird das Kennwort, der in der ID-Vault gespeicherten Benutzer-ID-Datei, durch das initiale Kennwort aus der One Identity Manager-Datenbank ersetzt. Ist der Benutzer zu diesem

Zeitpunkt am IBM Notes Client angemeldet, wird die lokale ID-Datei des Benutzers durch die aktualisierte Kopie aus der ID-Vault ersetzt. Beim nächsten Start des IBM Notes Clients muss der Benutzer sich mit dem initialen Kennwort anmelden. Ist der Benutzer nicht am IBM Notes Client angemeldet, während das Kennwort zurückgesetzt wird, muss die aktualisierte ID-Datei dem Benutzer separat zur Verfügung gestellt werden.

Sobald das Kennwort erfolgreich zurückgesetzt wurde, müssen dem Benutzer das initiale Kennwort sowie gegebenenfalls die ID-Datei zur Verfügung gestellt werden. Dieser Prozess ist kundenspezifisch zu implementieren.

ID-Restore

ID-Restore ist ein One Identity Manager-Mechanismus der verwendet werden kann, wenn ein Benutzer das Kennwort zu seiner ID-Datei vergessen beziehungsweise die ID-Datei selbst verloren hat. Wenn die Benutzer-ID-Datei über das ID-Restore-Verfahren wiederhergestellt wird, werden aus den Namensangaben des Benutzerkontos, der organisatorischen Einheit und dem Zertifikat der vollständige Name des Benutzerkontos und der Anzeigename ermittelt.

Um eine ID-Wiederherstellung durchzuführen, sind folgende Informationen notwendig:

- eine initial in die Datenbank importierte ID-Datei, inklusive zugehörigem Kennwort (`NDOUser.NotesID`, `NDOUser.PasswordInitial`)
- der Zertifizierer, mit dem die initiale ID-Datei erzeugt wurde (`NDOUser.UID_NDOCertifierInitial`)
- eine Kopie des initial eingelesenen beziehungsweise angelegten Personendokuments in der Archivdatenbank `archive.nsf` des Gateway Servers
- die GUID der Dokumentenkopie in der Archivdatenbank (`NDOUser.ObjectGUID_Archiv`)

Für Benutzerkonten, die im One Identity Manager angelegt wurden, werden diese Daten automatisiert generiert und gespeichert. Für alle anderen Benutzerkonten muss einmalig ein kundenspezifischer Import der oben genannten Daten durchgeführt werden.

Um die Benutzer-ID-Datei wiederherzustellen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto aus.
3. Wählen Sie die Aufgabe **ID-Restore**.

   Der Prozess zur ID-Wiederherstellung führt folgende Schritte aus:

   - Löschen des aktuellen Personendokuments aus dem Dominoverzeichnis.
   - Kopieren des initialen Personendokuments aus der Archivdatenbank in das Dominoverzeichnis.
   - Exportieren der initial gespeicherten ID-Datei auf den Gateway Server.
   - Einstellen des AdminP-Auftrages zum Nachführen der bisher auf der Original-ID durchgeführten Veränderungen. Dies beinhaltet Änderungen an

Namensbestandteilen des Benutzerkontos, Änderungen des ID-Ablaufdatums sowie Wechsel in andere Zertifizierer.

- Aktualisieren des wiederhergestellten Personendokuments mit den bekannten Werten.

4. Wenn die ID-Datei wiederhergestellt ist, stellen Sie dem Benutzer die ID-Datei und das initiale Kennwort zur Verfügung.

Verwandte Themen

- Anlegen einer Archivdatenbank zur Sicherung der Personendokumente auf Seite 24

Sperren und Entsperren von Notes Benutzerkonten

Tabelle 43: Konfigurationsparameter für das Sperren/Entsperren von Benutzerkonten

Konfigurationsparameter	Wirkung bei Aktivierung
TargetSystem\NDO\MailBoxAnonymPre	Angabe des Präfix für die Anonymisierung von Benutzerkonten
QER\Person\TemporaryDeactivation	Der Konfigurationsparameter legt fest, ob die Benutzerkonten der Person gesperrt werden, wenn die Person zeitweilig oder dauerhaft deaktiviert wird.

Ein Benutzerkonto gilt in einer IBM Notes-Umgebung dann als gesperrt, wenn der Benutzer keine Möglichkeit mehr hat, sich mit diesem Benutzerkonto an Servern der Domäne anzumelden. Dadurch verliert er auch den Zugriff auf seine Postfachdatei. Der Zugriff auf einen Server kann unterbunden werden, indem das Benutzerkonto auf dem entsprechenden Serverdokument den Berechtigungstyp "Not Access Server" erhält. In Umgebungen mit mehreren Servern ist dies sehr aufwändig, da ein zu sperrendes Benutzerkonto auf jedem Serverdokument diesen Berechtigungstyp erhalten muss.

Aus diesem Grund werden Sperrgruppen verwendet. Eine solche Sperrgruppe erhält zunächst auf jedem Serverdokument den Berechtigungstyp "Not Access Server". Ein Benutzer, der gesperrt werden soll, wird nur noch Mitglied der Sperrgruppe und hat somit automatisch keinen Zugriff mehr auf die Server der Domäne.

Wie Sie Benutzerkonten sperren, 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 gesperrt, 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 `NDOUser.AccountDisabled`.

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 gesperrt, 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 gesperrt, 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 sperren

1. Wählen Sie im Manager die Kategorie **IBM Notes | 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:

- Benutzerkonten sind nicht mit Personen verbunden.

Um ein Benutzerkonto zu sperren, das nicht mit einer Person verbunden ist

1. Wählen Sie im Manager die Kategorie **IBM Notes | 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.

Das Benutzerkonto wird beim Sperren anonymisiert, so dass es in den Adressbüchern nicht angezeigt wird. Es wird ihm der Zugriff auf die Notes Server entzogen. Bei dieser Anonymisierung des Benutzerkontos wird der Konfigurationsparameter "TargetSystem\NDO\MailBoxAnonymPre" ausgewertet.

Um ein Benutzerkonto zu entsperren

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Deaktivieren Sie auf dem Tabreiter **Allgemein** die Option **Benutzerkonto ist deaktiviert**.
5. Speichern Sie die Änderungen.

   Die Anonymisierung wird entfernt und das Benutzerkonto aus den Sperrgruppen entfernt.

Detaillierte Informationen zum Thema

- Sperrgruppen auf Seite 165

Verwandte Themen

- Einrichten von Kontendefinitionen auf Seite 47
- Erstellen der Automatisierungsgrade auf Seite 50

Löschen und Wiederherstellen von Notes Benutzerkonten

Wird ein Benutzerkonto im One Identity Manager gelöscht, wird es zunächst zum Löschen markiert. Das Benutzerkonto wird daraufhin gesperrt. Je nach Einstellung der Löschverzögerung wird das Benutzerkonto sofort oder zu einem späteren Zeitpunkt aus den Adressbüchern und aus der One Identity Manager-Datenbank gelöscht.

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.

Um ein Benutzerkonto zu löschen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie , um das Benutzerkonto zu löschen.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Um ein Benutzerkonto wiederherzustellen

1. Wählen Sie die Kategorie **IBM Notes | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste .

Konfigurieren der Löschverzögerung

Standardmäßig werden Benutzerkonten mit einer Löschverzögerung von 30 Tagen endgültig aus der Datenbank entfernt. Die Benutzerkonten werden zunächst deaktiviert. 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. Eine abweichende Löschverzögerung konfigurieren Sie im Designer an der Tabelle `NDOUser`.

Verwandte Themen

- Sperren und Entsperren von Notes Benutzerkonten auf Seite 140

9

Notes Gruppen

In Notes Gruppen können Benutzerkonten, Mail-In-Datenbanken, Gruppen und Server zusammengefasst werden. IBM Notes teilt Gruppen in verschiedene Gruppentypen ein. Der Gruppentyp spezifiziert den Zweck der Gruppe und entscheidet über die Sichtbarkeit der Gruppe im Domino-Verzeichnis.

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten von Notes Gruppen auf Seite 144

Allgemeine Stammdaten von Notes Gruppen

Tabelle 44: Konfigurationsparameter für die Risikobewertung von Benutzerkonten

Konfigurationsparameter	Wirkung bei Aktivierung
QER | CalculateRiskIndex	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Berechnung des Risikoindex. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren.

Konfigurationsparameter	Wirkung bei Aktivierung
	Ist der Parameter aktiviert, können Werte für den Risikoindex erfasst und berechnet werden.

Für Gruppen erfassen Sie folgende Stammdaten.

Tabelle 45: Allgemeine Stammdaten einer Notes Gruppe

Eigenschaft	Beschreibung
Gruppe	Name der Gruppe.
Anzeigename	Anzeigename der Gruppe.
Notes Domäne	Domäne, in der die Gruppe verwaltet wird.
Gruppentyp	Zweck der Gruppe. Der Gruppentyp entscheidet über die Sichtbarkeit der Gruppe im Domino-Verzeichnis. Anwendbare Gruppentypen sind: • 0 - Mehrere Zwecke • 1 - Nur Mail • 2 - Nur Zugriffskontrollliste • 3 - Nur Negativliste • 4 - Nur Server
Übergeordnete Notes Gruppe	Eindeutige Kennung der dynamischen Gruppe, zu der die Erweiterungsgruppe gehört. Diese Eigenschaft wird an allen Erweiterungsgruppen einer dynamischen Gruppe gepflegt.
Leistungsposition	Angabe einer Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
Internetadresse	Internet-E-Mail-Adresse der Gruppe.
Notes Kategorie	Angaben, um die Gruppe weiter zu kategorisieren. Um eine neue Notes Kategorie anzulegen, klicken Sie .
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Benutzerkonten. Stellen Sie 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.
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.

Eigenschaft	Beschreibung
	Ausführliche Informationen finden Sie im One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.
Dynamische Mitglieder einlesen	Methode zum Festlegen der Mitglieder einer dynamischen Gruppe. Wählen Sie "Home server", wenn die Gruppenmitglieder dynamisch aus den Mitgliedern des Homeservers ermittelt werden sollen. Für diese Gruppe werden die Ausschluss- und die Einschlussliste synchronisiert. Wählen Sie "Keine", wenn die Gruppe keine dynamische Gruppe ist.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Abgleich mit fremdem Verzeichnis erlaubt	Angabe, ob Informationen über diese Gruppe an fremde Verzeichnisse weitergeschickt werden dürfen.
Sperrgruppe	Angabe, ob die Gruppe als Sperrgruppe genutzt wird.
IT Shop	Angabe, 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. Die Option kann nicht aktiviert werden, wenn die Gruppe eine dynamische Gruppe ist. Ausführliche Informationen finden Sie im One Identity Manager Administrationshandbuch für IT Shop.
Verwendung nur im IT Shop	Angabe, 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.
Dynamische Gruppe	Angabe, ob es sich um eine dynamische Gruppe handelt. Diese Option wird abhängig von der Eigenschaft "Dynamische Mitglieder einlesen" gesetzt.

Detaillierte Informationen zum Thema

- Erweiterungsgruppen auf Seite 167
- Festlegen der Kategorien für die Vererbung von Notes Gruppen auf Seite 90
- Dynamische Gruppen auf Seite 167
- Sperrgruppen auf Seite 165

Notes Gruppen an Notes Benutzerkonten zuweisen

Gruppen können direkt oder indirekt an Personen zugewiesen werden. Bei der indirekten Zuweisung werden Personen und Gruppen in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der Gruppen, die einer Person zugewiesen ist. Wenn Sie eine Person in hierarchische Rollen aufnehmen und die Person ein Benutzerkonto besitzt, dann wird dieses Benutzerkonto in die Gruppe aufgenommen. Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind:

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und Gruppen erlaubt.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.
- Benutzerkonten und Gruppen gehören zur selben Domäne.

Des Weiteren können Gruppen über IT Shop-Bestellungen an Personen zugewiesen werden. Damit Gruppen über IT Shop-Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle Gruppen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Gruppen werden nach erfolgreicher Genehmigung den Personen zugewiesen.

Ausführliche Informationen zur Vererbung von Unternehmensressourcen finden Sie im One Identity Manager Administrationshandbuch für das Identity Management Basismodul.

Detaillierte Informationen zum Thema

- Notes Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 147
- Notes Gruppen an Geschäftsrollen zuweisen auf Seite 149
- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 150
- Notes Gruppen in Systemrollen aufnehmen auf Seite 151
- Notes Gruppen in den IT Shop aufnehmen auf Seite 151

Notes Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Gruppe an Abteilungen, Kostenstellen oder Standorte zu, damit sie über diese Organisationen an Benutzerkonten zugewiesen wird. Diese Aufgabe steht für dynamische Gruppen nicht zur Verfügung.

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

1. Wählen Sie im Manager die Kategorie **IBM Notes | Gruppen**.
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 **Notes 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

- Notes Gruppen an Geschäftsrollen zuweisen auf Seite 149
- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 150
- Notes Gruppen in Systemrollen aufnehmen auf Seite 151
- Notes Gruppen in den IT Shop aufnehmen auf Seite 151

- One Identity Manager Benutzer für die Verwaltung einer IBM Notes-Umgebung auf Seite 12

Notes Gruppen an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie Gruppen an Geschäftsrollen zu, damit sie über diese Geschäftsrollen an Benutzerkonten zugewiesen werden. Diese Aufgabe steht für dynamische Gruppen nicht zur Verfügung.

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

1. Wählen Sie im Manager die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** 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 **Notes Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu. Um die angezeigten Gruppen zu filtern, wählen Sie im Eingabefeld **Notes Domänen** eine Domäne aus.

   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

- Notes Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 147
- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 150
- Notes Gruppen in Systemrollen aufnehmen auf Seite 151
- Notes Gruppen in den IT Shop aufnehmen auf Seite 151
- One Identity Manager Benutzer für die Verwaltung einer IBM Notes-Umgebung auf Seite 12

Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Gruppen direkt an Benutzerkonten zuweisen. Diese Aufgabe steht für dynamische Gruppen nicht zur Verfügung.

Um eine Gruppe direkt an Benutzerkonten zuzuweisen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Mitglieder zuweisen**.
4. Wählen Sie den Tabreiter **Benutzer**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu. Um die angezeigten Benutzerkonten zu filtern, wählen Sie im Eingabefeld **Notes Domänen** eine Domäne aus.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Notes Gruppen direkt an ein Notes Benutzerkonto zuweisen auf Seite 122
- Notes Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 147
- Notes Gruppen an Geschäftsrollen zuweisen auf Seite 149
- Notes Gruppen in Systemrollen aufnehmen auf Seite 151
- Notes Gruppen in den IT Shop aufnehmen auf Seite 151
- Eigentümer an Notes Gruppen zuweisen auf Seite 163
- Administratoren an Notes Gruppen zuweisen auf Seite 164

Notes Gruppen in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

Mit dieser Aufgabe nehmen Sie eine Gruppe in Systemrollen auf. Wenn Sie eine Systemrolle an Personen zuweisen, wird die Gruppe an alle Benutzerkonten vererbt, die diese Personen besitzen. Diese Aufgabe steht für dynamische Gruppen nicht zur Verfügung.

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 **IBM Notes | Gruppen**.
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

- Notes Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 147
- Notes Gruppen an Geschäftsrollen zuweisen auf Seite 149
- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 150
- Notes Gruppen in den IT Shop aufnehmen auf Seite 151

Notes Gruppen in den IT Shop aufnehmen

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

- Die Gruppe ist keine dynamische Gruppe.
- Die Gruppe muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Gruppe muss eine Leistungsposition zugeordnet sein.

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien

zusammengestellt. Damit die Gruppe im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.

- Soll die Gruppe nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss die Gruppe 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 Gruppen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Gruppen in den IT Shop aufzunehmen.

Um eine Gruppe in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **IBM Notes | Gruppe** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | Notes Gruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppe an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Gruppe aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **IBM Notes | Gruppe** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | Notes Gruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppe aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Gruppe aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **IBM Notes | Gruppe** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | Notes Gruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe.

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

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

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

Verwandte Themen

- Allgemeine Stammdaten von Notes Gruppen auf Seite 144
- Notes Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 147
- Notes Gruppen an Geschäftsrollen zuweisen auf Seite 149
- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 150
- Notes Gruppen in Systemrollen aufnehmen auf Seite 151

Zusätzliche Aufgaben für die Verwaltung von Notes Gruppen

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

Überblick über die Notes Gruppe

Um einen Überblick über eine Gruppe zu erhalten

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die Notes Gruppe**.

Notes Mail-In-Datenbanken an eine Notes Gruppe zuweisen

Mail-In-Datenbanken können direkt an eine Gruppe zugewiesen werden.

Um Mail-In-Datenbanken an eine Gruppe zuzuweisen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Mitglieder zuweisen**.
4. Wählen Sie den Tabreiter **Mail-In-DB**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Mail-In-Datenbanken zu. Um die angezeigten Mail-In-Datenbanken zu filtern, wählen Sie im Eingabefeld **Notes Domänen** eine Domäne aus.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Mail-In-Datenbanken.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 150
- Notes Server an eine Notes Gruppe zuweisen auf Seite 154
- Notes Gruppen in Notes Gruppen aufnehmen auf Seite 155

Notes Server an eine Notes Gruppe zuweisen

Notes Server können direkt an eine Gruppe zugewiesen werden.

Um Server an eine Gruppe zuzuweisen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Mitglieder zuweisen**.
4. Wählen Sie den Tabreiter **Server**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Server zu. Um die angezeigten Server zu filtern, wählen Sie im Eingabefeld **Notes Domänen** eine Domäne aus.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Server.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 150
- Notes Mail-In-Datenbanken an eine Notes Gruppe zuweisen auf Seite 153
- Notes Gruppen in Notes Gruppen aufnehmen auf Seite 155

Notes Gruppen in Notes Gruppen aufnehmen

Einer Notes Gruppe können untergeordnete und übergeordnete Gruppen zugewiesen werden.

Um untergeordnete Gruppen an eine Gruppe zuzuweisen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Mitglieder zuweisen**.
4. Wählen Sie den Tabreiter **Gruppen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die untergeordneten Gruppen zu. Um die angezeigten Gruppen zu filtern, wählen Sie im Eingabefeld **Notes Domänen** eine Domäne aus.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die untergeordneten Gruppen.
6. Speichern Sie die Änderungen.

Um übergeordnete Gruppen an eine Gruppe zuzuweisen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Übergeordnete Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die übergeordneten Gruppen zu. Um die angezeigten Gruppen zu filtern, wählen Sie im Eingabefeld **Notes Domänen** eine Domäne aus.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die übergeordneten Gruppen.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 150
- Notes Server an eine Notes Gruppe zuweisen auf Seite 154
- Notes Mail-In-Datenbanken an eine Notes Gruppe zuweisen auf Seite 153

Wirksamkeit von Gruppenmitgliedschaften

Tabelle 46: Konfigurationsparameter für die bedingte Vererbung

Konfigurationsparameter	Wirkung bei Aktivierung
QER | Structures | Inherite | GroupExclusion	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Wirksamkeit von Gruppenmitgliedschaften. Ist der Parameter aktiviert, können aufgrund von Ausschlussdefinitionen die Gruppenmitgliedschaften reduziert werden. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.

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.
- Ob die Mitgliedschaft einer ausgeschlossenen Gruppe in einer anderen Gruppe zulässig ist (Tabelle NDOGroupInGroup), wird durch den One Identity Manager nicht überprüft.

Die Wirksamkeit der Zuweisungen wird in den Tabellen NDOUserInGroup und BaseTreeHasNDOGroup über die Spalte XIsInEffect abgebildet.

Beispiel für die Wirksamkeit von Gruppenmitgliedschaften

- In einer Domäne sind die Gruppen A, B und C definiert.
- 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 Domäne. 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 47: Festlegen der ausgeschlossenen Gruppen (Tabelle `NDOGroupExclusion`)

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

Tabelle 48: 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 49: 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.
- Sich ausschließende Gruppen gehören zur selben Domäne.

Um Gruppen auszuschließen

1. Wählen Sie im Manager die Kategorie **IBM Notes | Gruppen**.
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 Notes Gruppen anhand von Kategorien

Im One Identity Manager können Gruppen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen 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. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 31**.

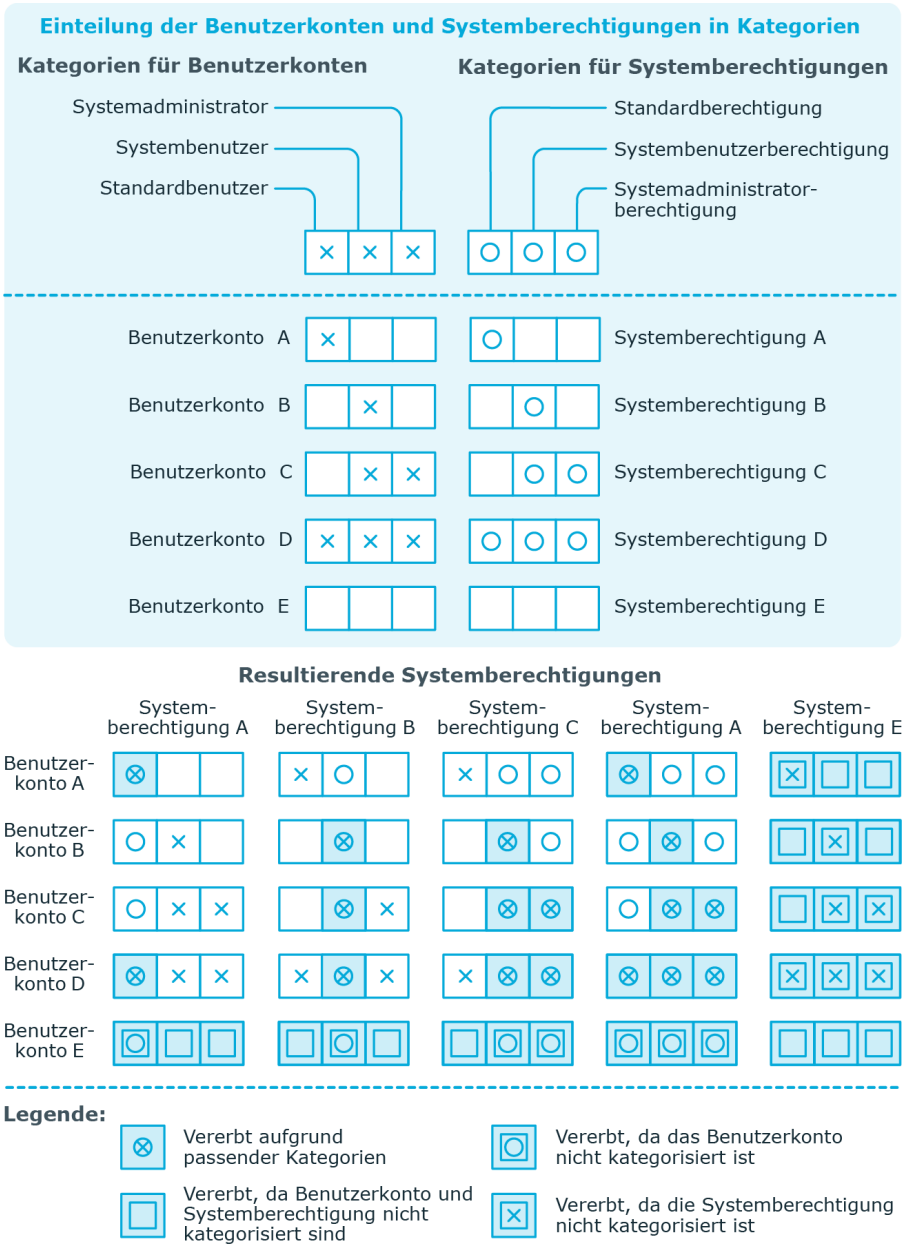
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto vererbt. Ist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

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

Tabelle 50: Beispiele für Kategorien

Kategorieposition	Kategorien für Benutzerkonten	Kategorien für Gruppen
1	Standardbenutzer	Standardberechtigung
2	Systembenutzer	Systembenutzerberechtigung
3	Systemadministrator	Systemadministratorberechtigung

Abbildung 2: Beispiel für die Vererbung über Kategorien



Um die Vererbung über Kategorien zu nutzen

- Definieren Sie an der Domäne die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Gruppen über ihre Stammdaten zu.

Verwandte Themen

- Festlegen der Kategorien für die Vererbung von Notes Gruppen auf Seite 90
- Allgemeine Stammdaten eines Notes Benutzerkontos auf Seite 111
- Allgemeine Stammdaten von Notes Gruppen auf Seite 144

Notes Gruppen als Eigentümer für Dokumente zuweisen

Legen Sie fest, für welche Dokumente eine Gruppe als Eigentümer eingetragen wird. Es können nur Dokumente zugewiesen werden, die zur selben Domäne gehören, wie die Gruppe.

Um eine Gruppe als Eigentümer für Benutzerkonten festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Dokumenteigentümer zuweisen**.
4. Wählen Sie den Tabreiter **Benutzer**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um eine Gruppe als Eigentümer für Gruppen festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Dokumenteigentümer zuweisen**.
4. Wählen Sie den Tabreiter **Gruppen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Um eine Gruppe als Eigentümer für Mail-In-Datenbanken festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Dokumenteigentümer zuweisen**.
4. Wählen Sie den Tabreiter **Mail In DB**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Mail-In-Datenbanken zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Mail-In-Datenbanken.
6. Speichern Sie die Änderungen.

Um eine Gruppe als Eigentümer für Zertifikate festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Dokumenteigentümer zuweisen**.
4. Wählen Sie den Tabreiter **Zertifikate**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zertifikate zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Zertifikate.
6. Speichern Sie die Änderungen.

Um eine Gruppe als Eigentümer für Server festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Dokumenteigentümer zuweisen**.
4. Wählen Sie den Tabreiter **Server**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Server zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Server.
6. Speichern Sie die Änderungen.

Notes Gruppen als Administrator für Dokumente zuweisen

Legen Sie fest, welche Dokumente eine Gruppe administrieren darf. Es können nur Dokumente zugewiesen werden, die zur selben Domäne gehören, wie die Gruppe.

Um eine Gruppe als Administrator für Benutzerkonten festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Administrierbare Dokumente zuweisen**.
4. Wählen Sie den Tabreiter **Benutzer**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um eine Gruppe als Administrator für Gruppen festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Administrierbare Dokumente zuweisen**.
4. Wählen Sie den Tabreiter **Gruppen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Um eine Gruppe als Administrator für Mail-In-Datenbanken festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Administrierbare Dokumente zuweisen**.
4. Wählen Sie den Tabreiter **Mail-In-DB**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Mail-In-Datenbanken zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Mail-In-Datenbanken.
6. Speichern Sie die Änderungen.

Um eine Gruppe als Administrator für Zertifikate festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Administrierbare Dokumente zuweisen**.
4. Wählen Sie den Tabreiter **Zertifikate**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zertifikate zu.

   - ODER -

Entfernen Sie im Bereich **Zuordnungen entfernen** die Zertifikate.

6. Speichern Sie die Änderungen.

Um eine Gruppe als Administrator für Serverdokumente festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Administrierbare Dokumente zuweisen**.
4. Wählen Sie den Tabreiter **Server Dokument**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Serverdokumente zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Serverdokumente.
6. Speichern Sie die Änderungen.

Um eine Gruppe als Administrator für Server festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Administrierbare Dokumente zuweisen**.
4. Wählen Sie den Tabreiter **Server**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Server zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Server.
6. Speichern Sie die Änderungen.

Eigentümer an Notes Gruppen zuweisen

Legen Sie fest, welche Benutzerkonten und Gruppen die ausgewählte Gruppe bearbeiten dürfen.

Um Benutzerkonten als Eigentümer für eine Gruppe festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Wählen Sie den Tabreiter **Benutzer**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Eigentümer für eine Gruppe festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Wählen Sie den Tabreiter **Gruppen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Administratoren an Notes Gruppen zuweisen

Legen Sie fest, welche Benutzerkonten und Gruppen die ausgewählte Notes Gruppe administrieren dürfen.

Um Benutzerkonten als Administratoren für eine Gruppe festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Administratoren zuweisen**.
4. Wählen Sie den Tabreiter **Benutzer**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Administratoren für eine Gruppe festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Administratoren zuweisen**.
4. Wählen Sie den Tabreiter **Gruppen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Zusatzeigenschaften an Notes Gruppen zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

Um Zusatzeigenschaften für eine Gruppe festzulegen

1. Wählen Sie im Manager die Kategorie **IBM Notes | Gruppen**.
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.

Ausführliche Informationen zur Einrichtung von Zusatzeigenschaften finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Sperrgruppen

Tabelle 51: Konfigurationsparameter für die Einrichtung von Sperrgruppen

Konfigurationsparameter	Wirkung bei Aktivierung
TargetSystem\NDO\DenyAccessGroups	Beim Sperren von Notes Benutzerkonten werden Sperrgruppen verwendet.
TargetSystem\NDO\DenyAccessGroups\Memberlimit	Der Konfigurationsparameter enthält die Maximalanzahl von Mitgliedern pro Sperrgruppe. Bei Erreichen dieses Limits wird automatisch eine weitere Sperrgruppe erzeugt.
TargetSystem\NDO\DenyAccessGroups\Prefix	Der Konfigurationsparameter enthält das Präfix, welches zur Bildung des Gruppennamens einer Sperrgruppe verwendet wird.

Ein Benutzerkonto gilt in einer IBM Notes-Umgebung dann als gesperrt, wenn der Benutzer keine Möglichkeit mehr hat, sich mit diesem Benutzerkonto an Servern der Domäne anzumelden. Dadurch verliert er auch den Zugriff auf seine Postfachdatei. Der Zugriff auf einen Server kann unterbunden werden, indem das Benutzerkonto auf dem entsprechenden Serverdokument den Berechtigungstyp "Not Access Server" erhält. In Umgebungen mit mehreren Servern ist dies sehr aufwändig, da ein zu sperrendes Benutzerkonto auf jedem Serverdokument diesen Berechtigungstyp erhalten muss.

Aus diesem Grund werden Sperrgruppen verwendet. Eine solche Sperrgruppe erhält zunächst auf jedem Serverdokument den Berechtigungstyp "Not Access Server". Ein Benutzer, der gesperrt werden soll, wird nur noch Mitglied der Sperrgruppe und hat somit automatisch keinen Zugriff mehr auf die Server der Domäne.

Sobald ein Benutzerkonto im One Identity Manager gesperrt wird, wird eine Sperrgruppe ermittelt, in der das Benutzerkonto Mitglied werden soll. Ist eine solche Sperrgruppe nicht vorhanden, wird vom One Identity Manager Service eine Gruppe mit dem Gruppentyp "Nur Negativliste" angelegt und automatisch mit dem Berechtigungstyp "Not Access Server" auf den einzelnen Servern versehen. Der Gruppenname besteht dabei aus einem Präfix und einem fortlaufenden Index (beispielsweise "viDenyAccess0001"). Des Weiteren wird diese Gruppe mit der Option **Sperrgruppe** gekennzeichnet.

Um das Präfix für Sperrgruppen zu ändern

1. Bearbeiten Sie im Designer den Wert des Konfigurationsparameters "TargetSystem\NDO\DenyAccessGroups\Prefix".
2. Erfassen Sie das Präfix, das beim Erstellen von Sperrgruppen verwendet werden soll.
3. Speichern Sie die Änderungen.

Es ist außerdem möglich, die maximale Anzahl von Benutzerkonten in einer Sperrgruppe festzulegen. Dies ist in Umgebungen mit einer sehr großen Menge an Benutzerkonten notwendig, um die maximale Anzahl der Benutzernamen in einer Gruppe nicht zu überschreiten. Wird dieses Limit erreicht, wird eine neue Sperrgruppe mit einem um den Wert "1" erhöhten Index angelegt und ebenfalls mit dem Berechtigungstyp "Not Access Server" auf sämtlichen Servern der Domäne eingetragen.

Um die zulässige Anzahl von Benutzerkonten in einer Sperrgruppe zu ändern

- Bearbeiten Sie im Designer den Wert des Konfigurationsparameters "TargetSystem\NDO\DenyAccessGroups\Memberlimit".

TIPP: Die Sperrgruppen werden durch das Skript `VI_Notes_GetOrCreateRestrictGroup` ermittelt und angelegt. Sind in einer IBM Notes-Umgebung bereits Sperrgruppen vorhanden, werden diese wie normale Gruppen behandelt.

Um diese Gruppen für Sperrprozesse im One Identity Manager zu verwenden

1. Aktivieren Sie für diese Gruppen die Option **Sperrgruppe**.
2. Passen Sie bei Bedarf das Präfix im Konfigurationsparameter "TargetSystem\NDO\DenyAccessGroups\Prefix" an.
3. Passen Sie das Skript `VI_Notes_GetOrCreateRestrictGroup` entsprechend Ihren Erfordernissen an.

Dynamische Gruppen

Seit der IBM Domino Version 8.5 ist es möglich, Benutzerkonten über bestimmte Auswahlkriterien an Gruppen zuzuweisen. Ein Kriterium ist beispielsweise der Mailserver eines Benutzerkontos. Benutzerkonten können darüber hinaus explizit aus einer Gruppe ausgeschlossen oder zusätzlich aufgenommen werden. Eine Gruppe wird im One Identity Manager als dynamische Gruppe abgebildet, wenn in der Eigenschaft "Dynamische Mitglieder einlesen" die Methode "Home server" ausgewählt ist (Spalte `AutoPopulateInput = '1'`). An diese Gruppen können keine Mitglieder direkt zugewiesen werden.

Dynamische Gruppen sind von der Vererbung über hierarchische Rollen ausgeschlossen. Damit können Systemrollen, Geschäftsrollen und Organisationen nicht an dynamische Gruppen zugewiesen werden. Es kann kein Vererbungsausschluss festgelegt werden. Dynamische Gruppen können nicht im IT Shop bestellt werden.

Erweiterungsgruppen

IBM Notes legt sogenannte Erweiterungsgruppen an, wenn die maximale Anzahl der Mitglieder einer dynamischen Gruppe erreicht ist. Diese Erweiterungsgruppen werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen, können jedoch nicht bearbeitet werden. Die Verbindung zur dynamischen Gruppe wird über die Eigenschaft **Übergeordnete Notes Gruppe** (Spalte `UID_NotesGroupParent`) hergestellt. Ausschluss- und Einschlusslisten werden ausschließlich an der übergeordneten dynamischen Gruppe gepflegt. Erweiterungsgruppen werden nur im Überblicksformular angezeigt.

Mitgliedschaften in dynamischen Gruppen

An dynamische Gruppen können keine Mitglieder direkt zugewiesen werden. Die Mitglieder werden über die Homeserver ermittelt, welche der Gruppe zugewiesen sind. Alle Benutzerkonten, denen einer dieser Server als Mailserver zugeordnet ist, sind automatisch Mitglied der dynamischen Gruppe. Zusätzlich können die Mitgliedschaften über eine Ausschluss- und eine Einschlussliste bearbeitet werden. Dabei werden Benutzerkonten, die sowohl der Ausschluss- als auch der Einschlussliste zugewiesen sind, nicht Mitglied der dynamischen Gruppe. Es können sowohl Benutzerkonten als auch Gruppen in die Ausschluss- und die Einschlussliste aufgenommen werden.

Bei der Berechnung der effektiven Mitglieder einer dynamischen Gruppe ermittelt IBM Notes alle Benutzerkonten,

- denen einer der Homeserver als Mailserver zugeordnet ist,
- die einer Einschlussliste direkt zugewiesen sind,
- die als Mitglied einer Notes Gruppe einer Einschlussliste zugewiesen sind,

- die einer Ausschlussliste zugewiesen sind,
- die als Mitglied einer Notes Gruppe einer Ausschlussliste zugewiesen sind.

Die effektiven Mitgliedschaften in dynamischen Gruppen (Tabelle NDOUserInGroup) werden nicht im One Identity Manager gepflegt, sondern nur durch die Synchronisation in die One Identity Manager eingelesen. Die Ausschluss- und die Einschlussliste können im Manager bearbeitet werden. Änderungen werden sofort in das Zielsystem provisioniert. Dort wird die Mitgliederliste neu berechnet. Nach erneuter Synchronisation sind die Änderungen an den effektiven Mitgliedschaften auch im One Identity Manager sichtbar und können beispielsweise bei Complianceprüfungen berücksichtigt werden.

Wenn Sie die Identity Audit Funktionalität des One Identity Manager nutzen und in den Complianceregeln auch Mitgliedschaften in dynamischen Notes Gruppen prüfen, beachten Sie folgenden Hinweis:

HINWEIS: Änderungen an der Einschluss- oder der Ausschlussliste im Manager können nicht sofort bei Complianceprüfungen berücksichtigt werden, da die effektiven Mitgliedschaften in den dynamischen Gruppen erst nach erneuter Synchronisation aktualisiert sind. Passen Sie den Zeitplan für die Synchronisation Ihrer IBM Notes-Umgebung so an, dass Änderungen an den effektiven Mitgliedschaften zeitnah in die One Identity Manager-Datenbank übertragen werden.

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

Zusätzliche Aufgaben für dynamische Gruppen

Um Mitgliedschaften in dynamischen Gruppen zu pflegen, können Sie auf dynamische Gruppen zusätzlich die folgenden Aufgaben anwenden. Die Aufgabe **Mitglieder zuweisen** steht nicht zur Verfügung.

Homeserver zuweisen

Einer dynamischen Gruppen können Sie Homeserver zuweisen. Alle Benutzerkonten, die einen dieser Server als Mailserver verwenden, sind dadurch Mitglied der dynamischen Gruppe.

Um Homeserver an eine dynamische Gruppe zuzuweisen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Gruppe.
3. Wählen Sie die Aufgabe **Homeserver zuweisen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Server zu. Um die angezeigten Server zu filtern, wählen Sie im Eingabefeld **Notes Domänen** eine Domäne aus.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Server.
5. Speichern Sie die Änderungen.

Ausschlussliste bearbeiten

Über die Ausschlussliste können Sie festlegen, welche Objekte aus der Mitgliederliste einer dynamischen Gruppe ausgeschlossen werden sollen.

Um Benutzerkonten aus einer dynamischen Gruppe auszuschließen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Gruppe.
3. Wählen Sie die Aufgabe **Ausschlussliste bearbeiten**.
4. Wählen Sie den Tabreiter **Benutzerkonten**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen aus einer dynamischen Gruppe auszuschließen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Gruppe.
3. Wählen Sie die Aufgabe **Ausschlussliste bearbeiten**.
4. Wählen Sie den Tabreiter **Gruppen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Um Server aus einer dynamischen Gruppe auszuschließen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Gruppe.
3. Wählen Sie die Aufgabe **Ausschlussliste bearbeiten**.
4. Wählen Sie den Tabreiter **Server**.

5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Server zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Server.
6. Speichern Sie die Änderungen.

Um Mail-In-Datenbanken aus einer dynamischen Gruppe auszuschließen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Gruppe.
3. Wählen Sie die Aufgabe **Ausschlussliste bearbeiten**.
4. Wählen Sie den Tabreiter **Mail-In-DB**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Mail-In-Datenbanken zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Mail-In-Datenbanken.
6. Speichern Sie die Änderungen.

Einschlussliste bearbeiten

Über die Einschlussliste können Sie festlegen, welche Objekte zusätzlich in die Mitgliederliste einer dynamischen Gruppe aufgenommen werden sollen.

Um Benutzerkonten zusätzlich in eine dynamische Gruppe aufzunehmen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Gruppe.
3. Wählen Sie die Aufgabe **Einschlussliste bearbeiten**.
4. Wählen Sie den Tabreiter **Benutzerkonten**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen zusätzlich in eine dynamische Gruppe aufzunehmen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Gruppe.
3. Wählen Sie die Aufgabe **Einschlussliste bearbeiten**.
4. Wählen Sie den Tabreiter **Gruppen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.

6. Speichern Sie die Änderungen.

Um Server zusätzlich in eine dynamische Gruppe aufzunehmen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Gruppe.
3. Wählen Sie die Aufgabe **Einschlussliste bearbeiten**.
4. Wählen Sie den Tabreiter **Server**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Server zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Server.
6. Speichern Sie die Änderungen.

Um Mail-In-Datenbanken zusätzlich in eine dynamische Gruppe aufzunehmen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die dynamische Gruppe.
3. Wählen Sie die Aufgabe **Einschlussliste bearbeiten**.
4. Wählen Sie den Tabreiter **Mail-In-DB**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Mail-In-Datenbanken zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Mail-In-Datenbanken.
6. Speichern Sie die Änderungen.

Löschen von Notes Gruppen

Um eine Gruppe zu löschen

1. Wählen Sie die Kategorie **IBM Notes | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Klicken Sie , um die Gruppe zu löschen.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Die Gruppe wird endgültig aus der One Identity Manager-Datenbank und der IBM Notes-Umgebung gelöscht.

Mail-In-Datenbanken

Um die Stammdaten einer Mail-In-Datenbank zu bearbeiten

1. Wählen Sie die Kategorie **IBM Notes | Mail-In-DB**.
2. Wählen Sie in der Ergebnisliste die Mail-In-Datenbank. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Mail-In-Datenbank.
4. Speichern Sie die Änderungen.

Allgemeine Stammdaten von Mail-In-Datenbanken

Für Mail-In-Datenbanken erfassen Sie die folgenden Stammdaten.

Tabelle 52: Stammdaten einer Mail-In-Datenbank

Eigenschaft	Beschreibung
Mail-In-Datenbank	Name der Mail-In-Datenbank.
Anzeigename	Anzeigename der Mail-In-Datenbank.
Notes Domäne	Domäne, in der die Mail-In-Datenbank verwaltet wird.
Notes Server	Vollständiger Name des Notes Servers, auf dem sich die Mail-In-Datenbank befindet.
Internetadresse	SMTP-Adresse im Format Maildatei@Organisation.Domäne.
Dateiname	Dateiname und Pfad der Mail-In-Datenbank relativ zum Domino-Verzeichnis.

Eigenschaft	Beschreibung
Nachrichtenspeicherung	Art der Nachrichtenspeicherung.
Abgleich mit fremdem Verzeichnis zulassen	Angabe, ob Einträge der Mail-In-Datenbank in fremden Verzeichnissen eingesehen werden können.
Eingehende Post verschlüsseln	Angabe, ob eingehende E-Mails verschlüsselt werden sollen.
Notes Schablone	Name der Schablone, die zum Erstellen der Mail-In-Datenbank genutzt wird.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Zusätzliche Aufgaben für Mail-In-Datenbanken

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

Überblick über die Mail-In-Datenbank

Um einen Überblick über eine Mail-In-Datenbank zu erhalten

1. Wählen Sie die Kategorie **IBM Notes | Mail-In-DB**.
2. Wählen Sie in der Ergebnisliste die Mail-In-Datenbank.
3. Wählen Sie die Aufgabe **Überblick über die Notes Mail-In-Datenbank**.

Notes Gruppen an eine Mail-In-Datenbank zuweisen

Um Berechtigungen für den Zugriff auf Mail-In-Datenbanken einzurichten, weisen Sie die Mail-In-Datenbanken an Notes Gruppen zu.

Um Gruppen an eine Mail-In-Datenbank zuzuweisen

1. Wählen Sie die Kategorie **IBM Notes | Mail-In-DB**.
2. Wählen Sie in der Ergebnisliste die Mail-In-Datenbank.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu. Um die angezeigten Gruppen zu filtern, wählen Sie im Eingabefeld **Notes Domänen** eine Domäne aus.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
5. Speichern Sie die Änderungen.

Eigentümer an eine Mail-In-Datenbank zuweisen

Für Mail-In-Datenbanken können Sie Eigentümerbeziehungen definieren. Dafür legen Sie fest, welche Benutzerkonten und Gruppen die Mail-In-Datenbank bearbeiten dürfen.

Um Benutzerkonten als Eigentümer festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Mail-In-DB**.
2. Wählen Sie in der Ergebnisliste die Mail-In-Datenbank.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Eigentümer festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Mail-In-DB**.
2. Wählen Sie in der Ergebnisliste die Mail-In-Datenbank.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Administratoren an eine Mail-In-Datenbank zuweisen

Für Mail-In-Datenbanken können Sie Administratorenbeziehungen definieren. Dafür legen Sie fest, welche Benutzerkonten und Gruppen die Mail-In-Datenbank administrieren dürfen.

Um Benutzerkonten als Administratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Mail-In-DB**.
2. Wählen Sie in der Ergebnisliste die Mail-In-Datenbank.
3. Wählen Sie die Aufgabe **Administratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Administratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Mail-In-DB**.
2. Wählen Sie in der Ergebnisliste die Mail-In-Datenbank.
3. Wählen Sie die Aufgabe **Administratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Ausschluss- und Einschlusslisten pflegen

Mail-In-Datenbanken können Mitglied dynamischer Gruppen sein. Über die Ausschlussliste legen Sie fest, welche Mail-In-Datenbanken aus der Mitgliederliste einer dynamischen Gruppe ausgeschlossen werden sollen. Über die Einschlussliste legen Sie fest, welche Mail-In-Datenbanken zusätzlich in die Mitgliederliste einer dynamischen Gruppe aufgenommen werden sollen.

Um eine Mail-In-Datenbanken in die Einschlussliste dynamischer Gruppen aufzunehmen

1. Wählen Sie die Kategorie **IBM Notes | Mail-In-DB**.
2. Wählen Sie in der Ergebnisliste die Mail-In-Datenbank.
3. Wählen Sie die Aufgabe **Ausschluss- und Einschlusslisten pflegen**.
4. Wählen Sie den Tabreiter **Einschlussliste**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die dynamischen Gruppen zu, in deren Mitgliederliste die Mail-In-Datenbank aufgenommen werden soll.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die dynamischen Gruppen.
6. Speichern Sie die Änderungen.

Um eine Mail-In-Datenbanken in die Ausschlussliste dynamischer Gruppen aufzunehmen

1. Wählen Sie die Kategorie **IBM Notes | Mail-In-DB**.
2. Wählen Sie in der Ergebnisliste die Mail-In-Datenbank.
3. Wählen Sie die Aufgabe **Ausschluss- und Einschlusslisten pflegen**.
4. Wählen Sie den Tabreiter **Ausschlussliste**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die dynamischen Gruppen zu, aus deren Mitgliederliste die Mail-In-Datenbank ausgeschlossen werden soll.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die dynamischen Gruppen.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Mitgliedschaften in dynamischen Gruppen auf Seite 167

11

Notes Server

Im One Identity Manager werden alle Server, die im Domino-Verzeichnis bekannt sind, als Notes Server abgebildet.

Um die Stammdaten eines Notes Servers zu bearbeiten

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Allgemeine Stammdaten von Notes Servern

Tabelle 53: Konfigurationsparameter für die Behandlung neuer Benutzer-ID-Dateien

Konfigurationsparameter	Wirkung bei Aktivierung
TargetSystem\NDO\StoreIDInAddressbook	Der Konfigurationsparameter regelt die Behandlung der ID-Dateien für neue Benutzerkonten. Ist der Konfigurationsparameter aktiviert, wird die erstellte ID-Datei als Attachment an das Personendokument angehängt. Ist der Konfigurationsparameter deaktiviert, wird die erstellte ID-Datei auf dem Gateway Server abgelegt.

Für Notes Server erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 54: Allgemeine Stammdaten eines Notes Servers

Eigenschaft	Beschreibung
Notes Server	Hierarchischer Name des Servers im Domino-Verzeichnis.
Titel	Zusätzliche Bezeichnungen des Servers. Es können mehrere Werte erfasst werden.
Notes Domäne	Notes Domäne, zu der der Server gehört.
Version	Notes Build-Version des Servers.
Pfad der Benutzer-ID-Dateien	Pfad auf dem Gateway Server, der zur Erstellung neuer Benutzer-ID-Dateien genutzt wird. Diese Angabe wird nur benötigt, wenn der Konfigurationsparameter "TargetSystem\NDO\StoreIDInAddressbook" deaktiviert ist.
Hat Notes Postfachdateien	Angabe, ob auf dem Server Postfachdateien verwaltet werden. Dieser Server wird als Mailserver beim Einrichten von Benutzerkonten zur Auswahl angeboten.
Pfad der Postfachdateien	Pfad zur Ablage der Postfachdateien relativ zum Datenverzeichnis. Diese Angabe wird nur benötigt, wenn die Option **Hat Notes Postfachdateien** aktiviert ist.
Serverdokument	Angabe, ob der Notes Server lediglich einem Serverdokument im Domino-Verzeichnis entspricht und physisch nicht existiert.
Clustername	Name des Clusters, wenn der Server zu einem Cluster gehört.
DNS Name des Servers	Vollständiger Name des Servers.
Internetkonfiguration aus Internet-Sites-Dokumenten laden	Angabe, ob die Internetprotokollkonfiguration aus den Internet-Sites-Dokumenten im Domino-Verzeichnis geladen werden. Wenn die Option deaktiviert ist, werden diese Informationen aus dem Serverdokument geladen.
SMTP-Service automatisch starten	Angabe, ob der SMTP-Service automatisch gestartet wird, wenn der Server gestartet wird.
Betriebssystem	Bezeichnung des installierten Betriebssystems.
Dauer für Formularausführung	Maximale Dauer für die Ausführung eines Formulars (in Sekunden).
Ist ID-Vault-Server	Angabe, ob dieser Server als ID-Vault-Server genutzt wird.

Standortdaten von Notes Servern

Auf dem Tabreiter **Standort** bearbeiten Sie die Standortdaten für Notes Server.

Tabelle 55: Standortdaten eines Notes Servers

Eigenschaft	Beschreibung
Telefonnummer	Telefonnumer, falls der Server Anrufe über ein Modem entgegen nehmen kann.
Zeitzonendifferenz	Lokale Zeitzone am Standort des Servers. Wird als Differenz zur koordinierten Weltzeit (UTC) angegeben.
Sommerzeit	Angabe, ob am Standort des Servers die Sommerzeit gilt.
Mailserver	Mailserver, der am Standort des Servers genutzt wird.
Durchgangsserver	Durchgangsserver, der am Standort des Servers genutzt wird. Entspricht dem Homeserver.

Auf dem Tabreiter **Kontakt** werden weitere Standortinformationen verwaltet.

Tabelle 56: Kontaktdaten eines Notes Servers

Eigenschaft	Beschreibung
Standort	Standort des Servers.
Abteilung	Abteilung des Servers.
Kommentar	Freitextfeld für zusätzliche Erläuterungen.
Detailbeschreibung	Freitextfeld für zusätzliche Erläuterungen.

Sicherheitseinstellungen von Notes Servern

Auf dem Tabreiter **Sicherheit** bearbeiten Sie die Sicherheitseinstellungen eines Servers.

Tabelle 57: Sicherheitseinstellungen eines Notes Servers

Eigenschaft	Beschreibung
Öffentliche Schlüssel vergleichen	Angabe, ob die öffentlichen Schlüssel aller Benutzer und Server überprüft werden müssen, sobald sie sich am Server anmelden.
Anonyme Verbindungen zulassen	Angabe, ob sich Benutzer und Server ohne gültiges Zertifikat am Server anmelden können.
Kennwörter von Notes-IDs überprüfen	Angabe, ob die Kennwörter der Benutzer-ID-Dateien geprüft werden, wenn sich Benutzer am Server anmelden.

Zusätzliche Aufgaben für die Verwaltung von Notes Servern

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

Überblick über den Notes Server

Um einen Überblick über einen Notes Server zu erhalten

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Überblick über den Notes Server**.

Gruppen an einen Notes Server zuweisen

Server können als Mitglieder in Gruppen aufgenommen werden.

Um einen Notes Server in Gruppen aufzunehmen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
5. Speichern Sie die Änderungen.

Mailserver an Benutzerkonten zuweisen

Notes Server können als Mailserver direkt an Benutzerkonten zugewiesen werden. Der Server wird an allen ausgewählten Benutzerkonten als Mailserver (Spalte `UID_NDOServer`) eingetragen. Die Aufgabe ist nur verfügbar, wenn an dem Server die Option **Hat Notes Postfachdateien** aktiviert ist.

Um einen Notes Server an Benutzerkonten zuzuweisen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten .
5. Speichern Sie die Änderungen.

Eigentümer an das Serverdokument zuweisen

Legen Sie fest, welche Benutzerkonten und Gruppen als Eigentümer des Serverdokuments eingetragen werden.

Um Benutzerkonten als Eigentümer für ein Serverdokument festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Dokumenteigentümer zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Eigentümer für ein Serverdokument festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Dokumenteigentümer zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Administratoren an das Serverdokument zuweisen

Legen Sie fest, welche Benutzerkonten und Gruppen das Serverdokument administrieren dürfen.

Um Benutzerkonten als Administratoren für ein Serverdokument festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Dokumentadministratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Administratoren für ein Serverdokument festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Dokumentadministratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Administratorzugriff festlegen

In der IBM Notes-Umgebung können die Zugriffsrechte der Administratoren eingeschränkt werden. Administratoren erhalten dabei die Berechtigungen nur auf bestimmte Zugriffsebenen. Sie können beispielsweise Datenbankadministratoren festlegen oder einzelnen Administratoren volle Berechtigungen erteilen.

Administratoren mit voller Berechtigung zuweisen

Weisen Sie die Benutzerkonten und Gruppen zu, die vollen Zugriff auf den Server erhalten sollen.

Um Benutzerkonten als Vollzugriffadministratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Vollzugriffadministratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Vollzugriffadministratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Vollzugriffadministratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Administratoren zuweisen

Legen Sie die Benutzerkonten und Gruppen fest, die den Server administrieren dürfen. Die Administratoren erhalten alle Rechte und Berechtigungen eines Datenbankadministrators und eines Administrators mit voller Remotekonsolenberechtigung.

Um Benutzerkonten als Administratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Administratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".

5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Administratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Administratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Datenbankadministratoren zuweisen auf Seite 184
- Administratoren mit voller Remotekonsolenberechtigung zuweisen auf Seite 185

Datenbankadministratoren zuweisen

Weisen Sie die Benutzerkonten und Gruppen zu, die Datenbanken auf dem Server verwalten sollen.

Um Benutzerkonten als Datenbankadministratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Datenbankadministratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Datenbankadministratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.

3. Wählen Sie die Aufgabe **Datenbankadministratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Administratoren mit voller Remotekonsolenberechtigung zuweisen

Weisen Sie die Benutzerkonten und Gruppen zu, die die Remotekonsole zum Ausführen von Befehlen an diesen Server verwenden dürfen. Das beinhaltet die Rechte und Berechtigungen eines leseberechtigten Administrators.

Um Benutzerkonten als Remotekonsolenadministratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Remotekonsolenadministratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als Remotekonsolenadministratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Remotekonsolenadministratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Leseberechtigte Administratoren zuweisen auf Seite 186

Leseberechtigte Administratoren zuweisen

Weisen Sie die Benutzerkonten und Gruppen zu, die die Remotekonsole nur zum Ausführen von Befehlen verwenden dürfen, die Systemstatusinformationen liefern.

Um Benutzerkonten als leseberechtigte Administratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Leseberechtigte Administratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als leseberechtigte Administratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Leseberechtigte Administratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Systemadministratoren zuweisen

Weisen Sie die Benutzerkonten und Gruppen zu, die sämtliche Betriebssystembefehle auf dem Server ausführen dürfen.

Um Benutzerkonten als Systemadministratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Systemadministratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.

6. Speichern Sie die Änderungen.

Um Gruppen als Systemadministratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Systemadministratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Eingeschränkte Systemadministratoren zuweisen auf Seite 187

Eingeschränkte Systemadministratoren zuweisen

Weisen Sie die Benutzerkonten und Gruppen zu, die nur beschränkte Betriebssystembefehle auf dem Server ausführen dürfen.

Um Benutzerkonten als eingeschränkte Systemadministratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Eingeschränkte Systemadministratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen als eingeschränkte Systemadministratoren festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Eingeschränkte Systemadministratoren zuweisen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".

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

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Systemadministratoren zuweisen auf Seite 186

Serverberechtigungen einrichten

Im Serverdokument werden Zugriffslisten definiert, die festlegen, welche Benutzer, Gruppen oder Server für verschiedene Zwecke Zugriff auf den Server erhalten.

Serverzugriff

Standardmäßig können alle Benutzerkonten, Gruppen und Server auf den Server zugreifen. Um den Serverzugriff einzuschränken, können Sie hier explizit die Benutzerkonten, Gruppen und Server zuweisen, die auf den Server zugreifen dürfen. Sobald Objekte zugewiesen sind, wird allen anderen Benutzerkonten, Gruppen und Servern der Serverzugriff verweigert.

Um nur einzelnen Benutzerkonten, Gruppen und Servern den Serverzugriff zu verweigern, nutzen Sie die Aufgabe **Kein Serverzugriff**. Weitere Informationen finden Sie unter Kein Serverzugriff auf Seite 189.

Um Benutzerkonten den Serverzugriff explizit zu gewähren

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Serverzugriff**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen den Serverzugriff explizit zu gewähren

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Serverzugriff**.

4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Um Servern den Serverzugriff explizit zu gewähren

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Serverzugriff**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Server".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Server zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Server.
6. Speichern Sie die Änderungen.

Kein Serverzugriff

Die angegebenen Benutzerkonten, Gruppen und Server können nicht auf den Server zugreifen. Wenn keine Benutzerkonten, Gruppen oder Server zugewiesen sind, können alle Benutzerkonten, Gruppen und Server, denen der Serverzugriff erlaubt ist, auf den Server zugreifen. Weitere Informationen finden Sie unter Serverzugriff auf Seite 188.

Um Benutzerkonten den Serverzugriff zu verweigern

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Kein Serverzugriff**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen den Serverzugriff zu verweigern

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Kein Serverzugriff**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".

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

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Um Servern den Serverzugriff zu verweigern

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Kein Serverzugriff**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Server".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Server zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Server.
6. Speichern Sie die Änderungen.

Datenbanken und Schablonen erstellen

Die angegebenen Benutzerkonten, Gruppen und Server können neue Datenbanken und Schablonen auf dem Server erstellen. Wenn keine Benutzerkonten, Gruppen oder Server zugewiesen sind, ist jedem die Erstellung neuer Datenbanken erlaubt.

Um Benutzerkonten zu erlauben, Datenbanken und Schablonen zu erstellen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Datenbanken und Schablonen erstellen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen zu erlauben, Datenbanken und Schablonen zu erstellen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Datenbanken und Schablonen erstellen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".

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

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Um Servern zu erlauben, Datenbanken und Schablonen zu erstellen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Datenbanken und Schablonen erstellen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Server".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Server zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Server.
6. Speichern Sie die Änderungen.

Neue Repliken erstellen

Die angegebenen Benutzerkonten, Gruppen und Server können Repliken von Datenbanken auf dem Server erstellen. Wenn keine Benutzerkonten, Gruppen oder Server zugewiesen sind, ist die Erstellung von Repliken nicht erlaubt.

Um Benutzerkonten zu erlauben, Repliken zu erstellen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Neue Repliken erstellen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen zu erlauben, Repliken zu erstellen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Neue Repliken erstellen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".

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

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Um Servern zu erlauben, Repliken zu erstellen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Neue Repliken erstellen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Server".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Server zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Server.
6. Speichern Sie die Änderungen.

Routing über Server

Die angegebenen Benutzerkonten, Gruppen und Server können den Server als Durchgangsserver nutzen, unabhängig davon, ob für sie der Serverzugriff gestattet ist. Wenn keine Benutzerkonten, Gruppen oder Server zugewiesen sind, ist der Server als Durchgangsserver nicht verfügbar.

Damit die Zuweisungen wirksam werden, müssen Server als Durchgangsziele eingerichtet sein. Weitere Informationen finden Sie unter Durchgangsziel für das Routing auf Seite 193.

Um Benutzerkonten zu erlauben, den Server als Durchgangsserver zu nutzen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Routing über Server**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen zu erlauben, den Server als Durchgangsserver zu nutzen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Routing über Server**.

4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Um Servern zu erlauben, den Server als Durchgangsserver zu nutzen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Routing über Server**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Server".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Server zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Server.
6. Speichern Sie die Änderungen.

Durchgangsziel für das Routing

Die angegebenen Benutzerkonten, Gruppen und Server können über einen Durchgangsserver auf diesen Server zugreifen. Für die Benutzerkonten, Gruppen und Server muss außerdem der Serverzugriff auf diesen Server eingerichtet sein.

Wenn keine Benutzerkonten, Gruppen oder Server zugewiesen sind, ist der Server als Durchgangsziel nicht verfügbar.

Um Benutzerkonten zu erlauben, den Server als Durchgangsziel zu nutzen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Auf diesen Server zugreifen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen zu erlauben, den Server als Durchgangsziel zu nutzen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Auf diesen Server zugreifen**.

4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Um Servern zu erlauben, den Server als Durchgangsziel zu nutzen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Auf diesen Server zugreifen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Server".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Server zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Server.
6. Speichern Sie die Änderungen.

Anruf durch Durchgangsserver veranlassen

Die angegebenen Benutzerkonten, Gruppen und Server können andere Server über diesen Durchgangsserver per Wählverbindung erreichen. Wenn keine Benutzerkonten, Gruppen oder Server zugewiesen sind, sind Anrufe nicht zulässig.

Damit die Zuweisungen wirksam werden, müssen Server als Durchgangsziele eingerichtet sein. Weitere Informationen finden Sie unter Durchgangsziel für das Routing auf Seite 193. Außerdem muss festgelegt sein, welche Benutzerkonten, Gruppen oder Server diesen Server als Durchgangsserver nutzen dürfen. Weitere Informationen finden Sie unter Routing über Server auf Seite 192.

Um Benutzerkonten zu erlauben, den Durchgangsserver für Wählverbindungen zu nutzen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Anruf veranlassen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen zu erlauben, den Durchgangsserver für Wählverbindungen zu nutzen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Anruf veranlassen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Um Servern zu erlauben, den Durchgangsserver für Wählverbindungen zu nutzen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Anruf veranlassen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Server".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Server zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Server.
6. Speichern Sie die Änderungen.

Zulässige Ziele für Durchgangsserver

Für einen Durchgangsserver können Sie die Zielserver angeben, die über diesen Durchgangsserver erreicht werden können. Ist kein Zielserver angegeben, kann auf alle Server, die als Durchgangsziel eingerichtet sind, zugegriffen werden.

Damit die Zuweisungen wirksam werden, müssen Server als Durchgangsziele eingerichtet sein. Weitere Informationen finden Sie unter Durchgangsziel für das Routing auf Seite 193. Außerdem muss festgelegt sein, welche Benutzerkonten, Gruppen oder Server diesen Server als Durchgangsserver nutzen dürfen. Weitere Informationen finden Sie unter Routing über Server auf Seite 192.

Um die Zielserver für einen Durchgangsserver festzulegen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Zulässige Ziele**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Server".

5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zielserver zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Zielserver.
6. Speichern Sie die Änderungen.

Unbeschränkte Methoden und Operationen signieren oder ausführen

Die angegebenen Benutzerkonten und Gruppen können auf dem Server alle Agenten ausführen, die mit ihrer Benutzer-ID-Datei signiert wurden. Die Rechte zum Ausführen beschränkter LotusScript- und Java-Agenten und zum Ausführen einfacher und Formel-Agenten sind damit eingeschlossen. Wenn keine Benutzerkonten und Gruppen zugewiesen sind, kann auf dem Server niemand diese Agenten ausführen.

Um Benutzerkonten zu gestatten, unbeschränkte Methoden und Operationen auszuführen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Unbeschränkte Methoden und Operationen signieren oder ausführen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen zu gestatten, unbeschränkte Methoden und Operationen auszuführen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Unbeschränkte Methoden und Operationen signieren oder ausführen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Beschränkte LotusScript/Java-Agenten ausführen auf Seite 197
- Einfache Agenten und Formel-Agenten ausführen auf Seite 198

Beschränkte LotusScript/Java-Agenten ausführen

Die angegebenen Benutzerkonten und Gruppen können auf dem Server einige LotusScript- und Java-Agenten ausführen. Wenn keine Benutzerkonten und Gruppen zugewiesen sind, kann auf dem Server niemand diese Agenten ausführen.

Um Benutzerkonten zu gestatten, beschränkte LotusScript/Java-Agenten auszuführen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Beschränkte LotusScript/Java-Agenten ausführen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen zu gestatten, beschränkte LotusScript/Java-Agenten auszuführen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Beschränkte LotusScript/Java-Agenten ausführen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Unbeschränkte Methoden und Operationen signieren oder ausführen auf Seite 196

Einfache Agenten und Formel-Agenten ausführen

Die angegebenen Benutzerkonten und Gruppen können auf dem Server (sowohl private als auch gemeinsame) einfache Agenten und Formel-Agenten ausführen. Wenn keine Benutzerkonten und Gruppen zugewiesen sind, können alle Benutzerkonten und Gruppen diese Agenten ausführen.

Um Benutzerkonten zu gestatten, einfache und Formel-Agenten auszuführen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Einfache und Formel-Agenten ausführen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Benutzerkonten".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
6. Speichern Sie die Änderungen.

Um Gruppen zu gestatten, einfache und Formel-Agenten auszuführen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Einfache und Formel-Agenten ausführen**.
4. Wählen Sie im Eingabefeld **Tabelle** die Tabelle "Notes Gruppen".
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Unbeschränkte Methoden und Operationen signieren oder ausführen auf Seite 196

Ausschluss- und Einschlusslisten pflegen

Notes Server können Mitglied dynamischer Gruppen sein. Über die Ausschlussliste legen Sie fest, welche Server aus der Mitgliederliste einer dynamischen Gruppe ausgeschlossen werden sollen. Über die Einschlussliste legen Sie fest, welche Server zusätzlich in die Mitgliederliste einer dynamischen Gruppe aufgenommen werden sollen.

Um einen Notes Server in die Einschlussliste dynamischer Gruppen aufzunehmen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Ausschluss- und Einschlusslisten pflegen**.
4. Wählen Sie den Tabreiter **Einschlussliste**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die dynamischen Gruppen zu, in deren Mitgliederliste der Server aufgenommen werden soll.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die dynamischen Gruppen.
6. Speichern Sie die Änderungen.

Um einen Notes Server in die Ausschlussliste dynamischer Gruppen aufzunehmen

1. Wählen Sie die Kategorie **IBM Notes | Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Ausschluss- und Einschlusslisten pflegen**.
4. Wählen Sie den Tabreiter **Ausschlussliste**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die dynamischen Gruppen zu, aus deren Mitgliederliste der Server ausgeschlossen werden soll.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die dynamischen Gruppen.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Mitgliedschaften in dynamischen Gruppen auf Seite 167

12

Nutzung von AdminP-Aufträgen zur Verarbeitung von IBM Notes Prozessen

IBM Notes verfügt über einen asynchronen Mechanismus zur Abarbeitung diverser interner Aufgaben. Wird beispielsweise der Name eines Benutzerkontos geändert, sorgt dieser Mechanismus dafür, dass die Zugriffssteuerungslisten von Notes Datenbanken ebenfalls angepasst werden.

Diese Aufgabe übernimmt der Notes Servertask „AdminP", der auf jedem Notes Server der Umgebung läuft. Dieser Task startet in gewissen Intervallen und prüft, ob neue Aufträge zur Abarbeitung vorliegen. Diese werden in Form von Anforderungsdokumenten in die Notes Datenbank `admin4.nsf` eingestellt und anschließend auf jeden Notes Server repliziert. Nach der Abarbeitung eines Auftrages erzeugt der ausführende Notes Server ein Antwortdokument sowie gegebenenfalls Folgeaufträge.

Bei einigen One Identity Manager Prozessen werden AdminP-Aufträge eingestellt, beispielsweise bei Änderungen von Namensbestandteilen eines Benutzerkontos, Zertifikatswechsel oder bei Wiederherstellung der Benutzer-ID.

Wann diese abgearbeitet werden, richtet sich nach mehreren Faktoren:

- Wann wurde der Auftrag auf den ausführenden Notes Server repliziert?
- In welchem Intervall läuft der AdminP-Servertask auf dem ausführenden Notes Server?
- Von welchem Typ ist der Auftrag?

Automatisches Bestätigen von AdminP-Aufträgen

Einige AdminP-Aufträge müssen zunächst vom Administrator bestätigt werden, bevor sie ausgeführt werden. Es ist mit dem One Identity Manager möglich, diese automatisch bestätigen zu lassen. Voraussetzung hierfür ist eine regelmäßige Synchronisation der Admin4-Datenbank.

Um offene AdminP-Aufträge regelmäßig bestätigen zu lassen

- Konfigurieren und aktivieren Sie im Designer den Zeitplan **IBM Notes Automatische Bestätigung von AdminP-Aufträgen**.

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

Bisher ist die Bestätigung der folgenden Aufträge implementiert:

- `Approve MailfileDeletion`
- `Approve MovedReplicaDeletion`
- `Approve ReplicaDeletion`

Stammdaten eines AdminP-Auftrags

Die Eigenschaften der synchronisierten AdminP-Aufträge werden im Manager angezeigt.

Um die Stammdaten eines Anforderungsdokuments anzuzeigen

- Wählen Sie die Kategorie **IBM Notes | Baumdarstellung | <Domäne> | AdminP-Aufträge | <Filter> | <Objekt> | <Aktion>**.

Tabelle 58: Stammdaten eines AdminP-Anforderungsdokuments

Eigenschaft	Beschreibung
Aktion	Aktion, die durch den AdminP-Auftrag ausgeführt werden soll.
Ausführender Server	Server, der den Auftrag ausführen soll.
Objekt	Name des Objekts, für das die Aktion ausgeführt werden soll.
Autor	Name des Autors des AdminP-Auftrags.
Datenbankdatei	Dateinamen der zu verarbeitenden Datenbanken.
Genehmigungskennzeichen	Angabe, ob der AdminP-Auftrag durch einen Administrator genehmigt wurde.
Änderungskennzeichen	Angabe, ob der AdminP-Auftrag geändert wurde.

Um die Stammdaten eines Antwortdokuments anzuzeigen

1. Wählen Sie die Kategorie **IBM Notes | Baumdarstellung | <Domäne> | AdminP-Aufträge | <Filter> | <Objekt> | <Aktion>**.
2. Wählen Sie in der Ergebnisliste das Antwortdokument.

Tabelle 59: Stammdaten eines AdminP-Antwortdokuments

Eigenschaft	Beschreibung
Aktion	Aktion, die durch den AdminP-Auftrag ausgeführt wurde.
Anforderungsdokument	Eindeutige Kennung des zugehörigen Anforderungsdokuments.
Objekt	Name des Objekts, das verarbeitet wurde.
Autor	Name des Autors des AdminP-Auftrags.
Ausführender Server	Server, der den Auftrag ausgeführt hat.
Auftrag erstellt am	Datum, an dem der Auftrag erstellt wurde.
Datenbankdatei	Dateinamen der verarbeiteten Datenbanken.
Fehlerkennzeichen	Angabe, ob bei der Verarbeitung des AdminP-Auftrags Fehler aufgetreten sind.

13

Berichte über Notes Domänen

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 Notes Domänen stehen folgende Berichte zur Verfügung.

Tabelle 60: Berichte für das Zielsystem

Bericht	Beschreibung
Übersicht aller Zuweisungen (Domäne)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die in der ausgewählten Domäne mindestens ein Benutzerkonto besitzen.
Übersicht aller Zuweisungen (Zertifikat)	Der Bericht zeigt alle Rollen, in denen sich Personen befinden, deren Notes Benutzerkonto mit dem ausgewählten Zertifikat erstellt wurde.
Übersicht aller Zuweisungen (Gruppe)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, welche die ausgewählte Gruppe besitzen.
Unverbundene Benutzerkonten anzeigen	Der Bericht zeigt alle Benutzerkonten der Domäne, denen keine Person zugeordnet ist. Der Bericht enthält die Gruppenmitgliedschaften und die Risikoeinschätzung.
Ungenutzte Benutzerkonten anzeigen	Der Bericht enthält alle Benutzerkonten der Domäne, die in den letzten Monaten nicht verwendet wurden. Der Bericht enthält die Gruppenmitgliedschaften und die Risikoeinschätzung.
Abweichende Systemberechtigungen anzeigen	Der Bericht enthält alle Gruppen der Domäne, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager.
Benutzerkonten mit einer überdurchschnittlichen Anzahl an Systemberechtigungen anzeigen	Der Bericht enthält alle Benutzerkonten der Domäne, die eine überdurchschnittliche Anzahl an Gruppenmitgliedschaften besitzen.
Personen mit mehreren	Der Bericht zeigt alle Personen, die mehrere Notes Benut-

Bericht	Beschreibung
Benutzerkonten anzeigen	zerkonten in der Domäne besitzen. Der Bericht enthält eine Risikoeinschätzung.
IBM Notes Benut-zerkonten- und Gruppen-verteilung	Der Bericht enthält eine Zusammenfassung zur Benut-zerkonten- und Gruppenverteilung aller Notes Domänen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager| Übersichten Zielsysteme**.
Datenqualität der IBM Notes Benutzerkonten	Der Bericht enthält verschiedenen Auswertungen zur Daten-qualität der Benutzerkonten aller Notes Domänen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager | Analyse Datenqualität**.

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 3: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 61: 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.

Anhang A

Konfigurationsparameter für die Synchronisation mit einer Notes Domäne

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

Tabelle 62: Konfigurationsparameter für die Synchronisation einer Notes Domäne

Konfigurationsparameter	Bedeutung bei Aktivierung
TargetSystem\NDO	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung des Zielsystems IBM Notes. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.
TargetSystem\NDO\Accounts	Parameter zur Konfiguration der Angaben zu Notes Benutzerkonten.
TargetSystem\NDO\Accounts\InitialRandomPassword	Der Konfigurationsparameter legt fest, 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\NDO\Accounts\InitialRandomPassword\SendTo	Angabe, welche Person die E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Ab-

Konfigurationsparameter	Bedeutung bei Aktivierung
	teilung/Standort/Geschäftsrolle, Verantwortlicher der Person oder `XUserInserted`). Ist kein Empfänger ermittelbar, dann wird die E-Mail an die im Konfigurationsparameter "TargetSystem\NDO\DefaultAddress" hinterlegt Adresse versandt.
TargetSystem\NDO\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den Anmeldeinformationen zum Benutzerkonto zu versorgen. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto** verwendet.
TargetSystem\NDO\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword	Der Konfigurationsparameter enthält den Namen 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\NDO\Accounts\MailTemplateDefaultValues	Der Konfigurationsparameter enthält die 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\NDO\BuildShortnameFullSync	Der Konfigurationsparameter legt fest, ob bei der Synchronisation Kurznamen für Personendokumente erzeugt werden sollen, die im IBM Notes keinen Kurznamen besitzen. Ist der Parameter aktiviert, werden Kurznamen erzeugt. Ist der Konfigurationsparameter deaktiviert, können Benutzerkonten ohne Kurznamen nicht in der One Identity Manager-Datenbank angelegt werden.
TargetSystem\NDO\CreateMailDB	Der Konfigurationsparameter legt fest,

Konfigurationsparameter	Bedeutung bei Aktivierung
	ob die Postfachdatei nach oder während der Registrierung des Notes Benutzers im Zielsystem erzeugt wird. Wenn der Konfigurationsparameter aktiviert ist, wird die Postfachdatei während der Registrierung erzeugt. Dabei wird die Schablone des Notes Servers verwendet, auf dem der Benutzer registriert wird. Wenn der Konfigurationsparameter deaktiviert ist (Standard), wird die Postfachdatei nach der Registrierung des Notes Benutzers erzeugt. Dabei wird die Schablone verwendet, die am Benutzerkonto oder im Konfigurationsparameter „TargetSystem\NDO\DefTemplatePath" angegeben ist.
TargetSystem\NDO\DefaultAddress	Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem\NDO\DefTemplatePath	Standardschablone zum Anlegen der Postfachdateien auf einem Notes Server.
TargetSystem\NDO\DenyAccessGroups	Parameter zur Konfiguration der Sperrgruppen für das Sperren von Benutzerkonten.
TargetSystem\NDO\DenyAccessGroups\Memberlimit	Angabe der maximalen Anzahl von Mitgliedern pro Sperrgruppe. Bei Erreichen dieses Limits wird automatisch eine weitere Sperrgruppe erzeugt.
TargetSystem\NDO\DenyAccessGroups\Prefix	Präfix, welches zur Bildung des Gruppennamens einer Sperrgruppe verwendet wird.
TargetSystem\NDO\IsNorthAmerican	Angabe, ob neu erzeugte ID-Dateien kompatibel zur US-amerikanischen und kanadischen IBM Notes Version sind. Ist der Konfigurationsparameter aktiviert, werden alle neu erzeugten Benutzer-ID-Dateien mit nordamerikanischer Verschlüsselungsstärke

Konfigurationsparameter	Bedeutung bei Aktivierung
	berechnet.
TargetSystem\NDO\MailBoxAnonymPre	Präfix für die Anonymisierung von Benutzerkonten.
TargetSystem\NDO\MailFilePath	Verzeichnis auf dem Mailserver, in dem die Postfachdateien der Benutzerkonten abgelegt werden.
TargetSystem\NDO\MaxFullsyncDuration	Der Konfigurationsparameter enthält die maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.
TargetSystem\NDO\MinPasswordLength	Angabe der minimalen Kennwortlänge, die in allen neu zu berechnenden Benutzer-ID-Dateien zu setzen ist.
TargetSystem\NDO\PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem\NDO\PersonAutoDisabledAccounts	Der Konfigurationsparameter legt fest, ob an gesperrte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem\NDO\PersonAutoFullsync	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem\NDO\PersonExcludeList	Der Konfigurationsparameter enthält eine Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (|)

Konfigurationsparameter	Bedeutung bei Aktivierung
	getrennten Liste, die als reguläres Suchmuster verarbeitet wird.
TargetSystem\NDO\StoreIDInAddressbook	Der Konfigurationsparameter regelt die Behandlung der ID-Dateien für neue Benutzerkonten. Ist der Konfigurationsparameter aktiviert, wird die erstellte ID-Datei als Attachment an das Personendokument angehängt. Ist der Konfigurationsparameter deaktiviert, wird die erstellte ID-Datei auf dem Gateway Server abgelegt.
TargetSystem\NDO\TempNetworkPath	Temporäres Verzeichnis, in welchem neu erstellte ID-Dateien und persönliche Adressbücher abgelegt werden.
TargetSystem\NDO\UpdateAddressbook	Ist der Konfigurationsparameters aktiviert, werden beim Erzeugen neuer Benutzer-ID-Dateien auch Einträge im Domino-Verzeichnis erzeugt.
TargetSystem\NDO\UserType	Der Konfigurationsparameter legt den Typ des Benutzers fest, der durch eine Registrierung entsteht.
TargetSystem\NDO\VerifyUpdates	Der Konfigurationsparameter legt fest, ob bei einem Update geänderte Eigenschaften im Zielsystem überprüft werden. Ist der Parameter aktiviert, werden nach jedem Update die Eigenschaften des Objektes im Zielsystem verifiziert.

Anhang B

Standardprojektvorlage für IBM Notes

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 Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 63: Abbildung der Notes Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im IBM Notes	Tabelle im One Identity Manager Schema
AdminRequest	NDOAdmin4
Certifier	NDOCertifier
CertificateRequest	NDOCertifierRequest
Database	NDOMailInDB
CurrentDomain	NDODomain
Group	NDOGroup
Person	NDOUser
PolicyMaster	NDOPolicy
PolicyArchive	NDOPolicySetting
PolicyDesktop	NDOPolicySetting
PolicyMail	NDOPolicySetting

Schematyp im IBM Notes	Tabelle im One Identity Manager Schema
PolicyRegistration	NDOPolicySetting
PolicySecurity	NDOPolicySetting
PolicySetup	NDOPolicySetting
Server	NDOServer
Template	NDOTemplate

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

Index

C

D

E

G

I

J

K

L

M

N

O

P

R

S

V

Z