One Identity Manager 9.1

Administrationshandbuch für die Anbindung einer HCL Domino Umgebung

Copyright 2022 One Identity LLC.

ALLE RECHTE VORBEHALTEN.

Diese Anleitung enthält urheberrechtlich geschützte Informationen. Die in dieser Anleitung beschriebene Software wird unter einer Softwarelizenz oder einer Geheimhaltungsvereinbarung bereitgestellt. Diese Software darf nur in Übereinstimmung mit den Bestimmungen der geltenden Vereinbarung verwendet oder kopiert werden. Kein Teil dieser Anleitung darf ohne die schriftliche Erlaubnis von One Identity LLC in irgendeiner Form oder mit irgendwelchen Mitteln, elektronisch oder mechanisch reproduziert oder übertragen werden, einschließlich Fotokopien und Aufzeichnungen für irgendeinen anderen Zweck als den persönlichen Gebrauch des Erwerbers.

Die Informationen in diesem Dokument werden in Verbindung mit One Identity Produkten bereitgestellt. Durch dieses Dokument oder im Zusammenhang mit dem Verkauf von One Identity LLC Produkten wird keine Lizenz, weder ausdrücklich oder stillschweigend, noch durch Duldung oder anderweitig, an jeglichem geistigen Eigentumsrecht eingeräumt. MIT AUSNAHME DER IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT GENANNTEN BEDINGUNGEN ÜBERNIMMT ONE IDENTITY KEINERLEI HAFTUNG UND SCHLIESST JEGLICHE AUSDRÜCKLICHE, IMPLIZIERTE ODER GESETZLICHE GEWÄHRLEISTUNG ODER GARANTIE IN BEZUG AUF IHRE PRODUKTE AUS, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE IMPLIZITE GEWÄHRLEISTUNG DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET ONE IDENTITY FÜR JEGLICHE DIREKTE, INDIREKTE, FOLGE-, STÖRUNGS-, SPEZIELLE ODER ZUFÄLLIGE SCHÄDEN (EINSCHLIESSLICH, OHNE EINSCHRÄNKUNG, SCHÄDEN FÜR VERLUST VON GEWINNEN, GESCHÄFTSUNTERBRECHUNGEN ODER VERLUST VON INFORMATIONEN), DIE AUS DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DIESES DOKUMENTS RESULTIEREN, SELBST WENN ONE IDENTITY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN HAT. One Identity übernimmt keinerlei Zusicherungen oder Garantien hinsichtlich der Richtigkeit und Vollständigkeit des Inhalts dieses Dokuments und behält sich das Recht vor, Änderungen an Spezifikationen und Produktbeschreibungen jederzeit ohne vorherige Ankündigung vorzunehmen. One Identity verpflichtet sich nicht, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Wenn Sie Fragen zu Ihrer potenziellen Nutzung dieses Materials haben, wenden Sie sich bitte an:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Besuchen Sie unsere Website (http://www.OneIdentity.com) für regionale und internationale Büro-Adressen.

Patente

One Identity ist stolz auf seine fortschrittliche Technologie. Für dieses Produkt können Patente und anhängige Patente gelten. Für die aktuellsten Informationen über die geltenden Patente für dieses Produkt besuchen Sie bitte unsere Website unter http://www.OneIdentity.com/legal/patents.aspx.

Marken

One Identity und das One Identity Logo sind Marken und eingetragene Marken von One Identity LLC. in den USA und anderen Ländern. Für eine vollständige Liste der One Identity Marken, besuchen Sie bitte unsere Website unter www.OneIdentity.com/legal/trademark-information.aspx. Alle anderen Marken sind Eigentum der jeweiligen Besitzer.

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 HCL Domino Umgebung
Aktualisiert - 19. September 2022, 12:25 Uhr

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

Inhalt

Verwalten einer HCL Domino-Umgebung **10**
Architekturüberblick 11
One Identity Manager Benutzer für die Verwaltung einer Domino-Umgebung 13
Konfigurationsparameter für die Verwaltung von Domino-Umgebungen 15

Synchronisieren einer Domino-Umgebung **16**
Einrichten der Initialsynchronisation einer Domino-Umgebung 17
Benutzer und Berechtigungen für die Synchronisation mit einer Domino-Umgebung 18
Konfiguration des Domino-Servers 20
Einrichten eines Gateway Servers 20
Systemanforderungen für den Gateway Servers 21
Notes Client konfigurieren 22
Notes Zertifikate übernehmen 23
Kundenspezifische INI-Datei erstellen 23
One Identity Manager Service auf dem Gateway Server installieren 24
Archivdatenbank zur Sicherung der Personendokumente anlegen 27
Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Notes Domäne 28
Benötigte Informationen für die Erstellung eines Notes Synchronisationsprojektes .. 28
Initiales Synchronisationsprojekt für eine Notes Domäne erstellen 31
Synchronisationsprotokoll konfigurieren 34
Anpassen der Synchronisationskonfiguration für Domino-Umgebungen 35
Synchronisation in die Domino-Umgebung konfigurieren 36
Synchronisation verschiedener Notes Domänen konfigurieren 37
Einstellungen der Systemverbindung zur Notes Domäne ändern 37
Verbindungsparameter im Variablenset bearbeiten 38
Eigenschaften der Zielsystemverbindung bearbeiten 39
Schema aktualisieren 40
Beschleunigung der Synchronisation durch Revisionsfilterung 41
Provisionierung von Mitgliedschaften konfigurieren 42
Einzelobjektsynchronisation konfigurieren 44
Beschleunigung der Einzelobjektsynchronisation 45

Benutzertyp festlegen ... 46
Postfachdateien erzeugen ... 47
Benutzer-ID-Dateien erzeugen und speichern ... 48
Ausführen einer Synchronisation ... 50
Synchronisationen starten ... 50
Synchronisationsergebnisse anzeigen ... 51
Synchronisation deaktivieren ... 52
Einzelobjekte synchronisieren ... 53
Aufgaben nach einer Synchronisation ... 54
Ausstehende Objekte nachbearbeiten ... 54
Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen ... 56
Notes Benutzerkonten über Kontendefinitionen verwalten ... 57
Fehleranalyse ... 57
Datenfehler bei der Synchronisation ignorieren ... 58
Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) ... 59

Managen von Notes Benutzerkonten und Personen ... 61
Kontendefinitionen für Notes Benutzerkonten ... 62
Notes Kontendefinitionen erstellen ... 63
Notes Kontendefinitionen bearbeiten ... 64
Stammdaten von Notes Kontendefinitionen ... 64
Automatisierungsgrade bearbeiten ... 67
Automatisierungsgrade erstellen ... 68
Automatisierungsgrade an Notes Kontendefinitionen zuweisen ... 68
Stammdaten von Automatisierungsgraden ... 69
Abbildungsvorschriften für IT Betriebsdaten erstellen ... 70
IT Betriebsdaten erfassen ... 72
IT Betriebsdaten ändern ... 73
Zuweisen der Notes Kontendefinition an Personen ... 74
Notes Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen ... 75
Notes Kontendefinitionen an Geschäftsrollen zuweisen ... 76
Notes Kontendefinitionen an alle Personen zuweisen ... 76
Notes Kontendefinitionen direkt an Personen zuweisen ... 77
Notes Kontendefinitionen an Systemrollen zuweisen ... 77
Notes Kontendefinitionen in den IT Shop aufnehmen ... 78
Notes Kontendefinitionen an Zielsysteme zuweisen ... 80

Notes Kontendefinitionen löschen ... 81
Automatische Zuordnung von Personen zu Notes Benutzerkonten ... 83
Suchkriterien für die automatische Personenzuordnung bearbeiten ... 86
Personen suchen und direkt an Benutzerkonten zuordnen ... 87
Automatisierungsgrad an Notes Benutzerkonten ändern ... 89
Kontendefinitionen an verbundene Benutzerkonten zuweisen ... 89
Personen manuell mit Notes Benutzerkonten verbinden ... 90
Unterstützte Typen von Benutzerkonten ... 90
Standardbenutzerkonten ... 92
Administrative Benutzerkonten ... 93
Administrative Benutzerkonten für eine Person bereitstellen ... 94
Administrative Benutzerkonten für mehrere Personen bereitstellen ... 95
Privilegierte Benutzerkonten ... 96
Löschverzögerung für Notes Benutzerkonten festlegen ... 97

Managen von Mitgliedschaften in Notes Gruppen ... 99
Zuweisen von Notes Gruppen an Notes Benutzerkonten ... 99
Voraussetzungen für indirekte Zuweisungen von Notes Gruppen an Notes Benutzerkonten ... 100
Notes Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen ... 102
Notes Gruppen an Geschäftsrollen zuweisen ... 103
Notes Gruppen in Systemrollen aufnehmen ... 104
Notes Gruppen in den IT Shop aufnehmen ... 105
Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen ... 107
Notes Gruppen direkt an ein Notes Benutzerkonto zuweisen ... 108
Wirksamkeit von Mitgliedschaften in Notes Gruppen ... 109
Vererbung von Notes Gruppen anhand von Kategorien ... 111
Übersicht aller Zuweisungen ... 114

Bereitstellen von Anmeldeinformationen für Notes Benutzerkonten ... 116
Kennwortrichtlinien für Notes Benutzerkonten ... 116
Vordefinierte Kennwortrichtlinien ... 117
Kennwortrichtlinien anwenden ... 118
Kennwortrichtlinien erstellen ... 120
Kennwortrichtlinien bearbeiten ... 120
Allgemeine Stammdaten für Kennwortrichtlinien ... 121
Richtlinieneinstellungen ... 121

Zeichenklassen für Kennwörter 123
Kundenspezifische Skripte für Kennwortanforderungen 124
Skript zum Prüfen eines Kennwortes 125
Skript zum Generieren eines Kennwortes 126
Ausschlussliste für Kennwörter 127
Kennwörter prüfen 128
Generieren eines Kennwortes testen 128
Initiales Kennwort für neue Notes Benutzerkonten 128
E-Mail-Benachrichtigungen über Anmeldeinformationen 129

Nutzung von AdminP-Aufträgen zur Verarbeitung von Domino-Prozessen 131
AdminP-Aufträge automatisch bestätigen 132
Stammdaten von AdminP-Aufträgen 132

Abbilden von Notes Objekten im One Identity Manager 134
Notes Domänen 134
Stammdaten von Notes Domänen bearbeiten 135
Allgemeine Stammdaten für Notes Domänen 135
Kategorien für die Vererbung von Notes Gruppen definieren 137
Synchronisationsprojekt für eine Notes Domäne bearbeiten 138
Notes Benutzerkonten 138
Notes Benutzerkonten erstellen und bearbeiten 139
Allgemeine Stammdaten für Notes Benutzerkonten 141
E-Mail-System von Notes Benutzerkonten 145
Adressangaben von Notes Benutzerkonten 147
Zusätzliche Stammdaten von Notes Benutzerkonten 147
Administrative Daten von Notes Benutzerkonten 149
Zusatzeigenschaften an Notes Benutzerkonten zuweisen 151
Notes Benutzerkonten als Eigentümer für Dokumente festlegen 152
Eigentümer an Notes Benutzerkonten zuweisen 154
Notes Benutzerkonten als Administrator für Dokumente festlegen 155
Administratoren an Notes Benutzerkonten zuweisen 157
Ausschlusslisten und Einschlusslisten für Notes Benutzerkonten pflegen 158
Überblick über Notes Benutzerkonten anzeigen 159
Wiederherstellen der Benutzer-ID-Dateien 159
Benutzer-ID-Dateien über ID-Vault wiederherstellen 159

Benutzer-ID-Dateien über ID-Restore wiederherstellen ... 161
Notes Benutzerkonten sperren und entsperren ... 162
Notes Benutzerkonten löschen und wiederherstellen ... 164
Notes Gruppen ... 165
Notes Gruppen erstellen ... 166
Stammdaten für Notes Gruppen bearbeiten ... 166
Allgemeine Stammdaten von Notes Gruppen ... 166
Notes Mail-In-Datenbanken an Notes Gruppen zuweisen ... 168
Notes Server an Notes Gruppen zuweisen ... 169
Notes Gruppen in Notes Gruppen aufnehmen ... 170
Notes Gruppen als Eigentümer für Dokumente festlegen ... 171
Notes Gruppen als Administrator für Dokumente festlegen ... 173
Eigentümer an Notes Gruppen zuweisen ... 175
Administratoren an Notes Gruppen zuweisen ... 176
Zusatzeigenschaften an Notes Gruppen zuweisen ... 176
Überblick über Notes Gruppen anzeigen ... 177
Sperrgruppen ... 177
Dynamische Gruppen ... 178
Erweiterungsgruppen ... 179
Mitgliedschaften in dynamischen Gruppen ... 179
Homeserver zuweisen ... 180
Ausschlussliste bearbeiten ... 180
Einschlussliste bearbeiten ... 182
Notes Gruppen löschen ... 183
Notes Zertifikate ... 184
Stammdaten für Notes Zertifikate bearbeiten ... 184
Allgemeine Stammdaten für Notes Zertifikate ... 185
Kontaktdaten von Notes Zertifikaten ... 186
Eigentümer an Notes Zertifikate zuweisen ... 186
Administratoren an Notes Zertifikate zuweisen ... 187
Überblick über Notes Zertifikate anzeigen ... 188
Neu eingelesene Notes Zertifikate nachbehandeln ... 188
Notes Zertifikatsanforderungen anzeigen ... 189
Notes Schablonen ... 189
Notes Richtlinien ... 190

Stammdaten von Notes Richtlinien anzeigen 191
Stammdaten für Notes Richtlinien 191
Notes Richtlinieneinstellungen anzeigen 192
Mitglieder an Notes Richtlinien zuweisen 192
Eigentümer an Notes Richtlinien zuweisen 193
Administratoren an Notes Richtlinien zuweisen 194
Überblick über Notes Richtlinien anzeigen 195
Notes Mail-In-Datenbanken 195
Notes Mail-In-Datenbanken erstellen 196
Stammdaten für Notes Mail-In-Datenbanken bearbeiten 196
Allgemeine Stammdaten von Notes Mail-In-Datenbanken 197
Mail-In-Datenbanken an Notes Gruppen zuweisen 197
Eigentümer an Notes Mail-In-Datenbanken zuweisen 198
Administratoren an Notes Mail-In-Datenbanken zuweisen 199
Ausschlusslisten und Einschlusslisten für Notes Mail-In-Datenbanken pflegen 200
Überblick über Notes Mail-In-Datenbanken anzeigen 201
Notes Mail-In-Datenbanken löschen 201
Notes Server 201
Stammdaten für Notes Server bearbeiten 202
Allgemeine Stammdaten von Notes Servern 203
Standortdaten von Notes Servern 204
Sicherheitseinstellungen von Notes Servern 205
Notes Server an Notes Gruppen zuweisen 205
Mailserver an Notes Benutzerkonten zuweisen 206
Eigentümer an Serverdokumente zuweisen 207
Administratoren an Serverdokumente zuweisen 208
Administratorzugriff festlegen 208
Administratoren mit voller Berechtigung an Notes Server zuweisen 209
Administratoren an Notes Server zuweisen 210
Datenbankadministratoren an Notes Server zuweisen 211
Administratoren mit voller Remotekonsolenberechtigung an Notes Server zuweisen 212
Leseberechtigte Administratoren an Notes Server zuweisen 213
Systemadministratoren an Notes Server zuweisen 214
Eingeschränkte Systemadministratoren an Notes Server zuweisen 215

Serverberechtigungen für Notes Server einrichten ... 216
Serverzugriff zulassen ... 216
Serverzugriff einschränken ... 217
Datenbanken und Schablonen erstellen ... 218
Neue Repliken erstellen ... 220
Routing über Server zulassen ... 221
Notes Server als Durchgangsziele für das Routing einrichten ... 222
Anruf durch Durchgangsserver veranlassen ... 224
Zulässige Ziele für Durchgangsserver ... 225
Unbeschränkte Methoden und Operationen signieren oder ausführen ... 226
Beschränkte LotusScript/Java-Agenten ausführen ... 227
Einfache Agenten und Formel-Agenten ausführen ... 228
Ausschlusslisten und Einschlusslisten pflegen ... 229
Überblick über Notes Server anzeigen ... 230
Notes Server löschen ... 230
Berichte über Notes Objekte ... 230

Behandeln von Notes Objekten im Web Portal ... 234

Basisdaten für die Verwaltung einer Domino-Umgebung ... 236
Jobserver für Domino-spezifische Prozessverarbeitung ... 237
Allgemeine Stammdaten für Jobserver ... 238
Festlegen der Serverfunktionen ... 241
Zielsystemverantwortliche für Domino-Umgebungen ... 242

Anhang: Konfigurationsparameter für die Verwaltung einer Domino-Umgebung ... 246

Anhang: Standardprojektvorlage für Domino ... 249

Anhang: Verarbeitungsmethoden von Domino Systemobjekten ... 251

Anhang: Einstellungen des Domino Konnektors ... 253

Über uns ... 256

Kontaktieren Sie uns ... 257

Technische Supportressourcen ... 258

Index ... 259

1

Verwalten einer HCL Domino-Umgebung

Mit dem One Identity Manager werden die Objekte einer HCL Domino-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 Domino-Umgebungen parallel mit einer One Identity Manager-Datenbank möglich. Benutzer und Personendokumente werden im One Identity Manager als Notes Benutzerkonten verwaltet. Die Objekte des Domino-Verzeichnisses werden im One Identity Manager als Notes Objekte abgebildet.

HINWEIS: Der One Identity Manager unterstützt die Synchronisation mit verschiedenen Domino Versionen, beispielsweise HCL Domino Server Version 11 und IBM Domino Server Version 10. Da die Verwaltung der Objekte im One Identity Manager unabhängig von der Version der Zielsystemumgebung ist, wird auf das Zielsystem im One Identity Manager einheitlich mit der Bezeichnung Domino Bezug genommen.

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 zur Verfügung stehen müssen. Beim Anlegen eines Benutzers durch den Domino 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.

HINWEIS: Voraussetzung für die Verwaltung einer Domino-Umgebung im One Identity Manager ist die Installation des Domino Moduls. Ausführliche Informationen zur Installation finden Sie im *One Identity Manager Installationshandbuch.*

Architekturüberblick

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

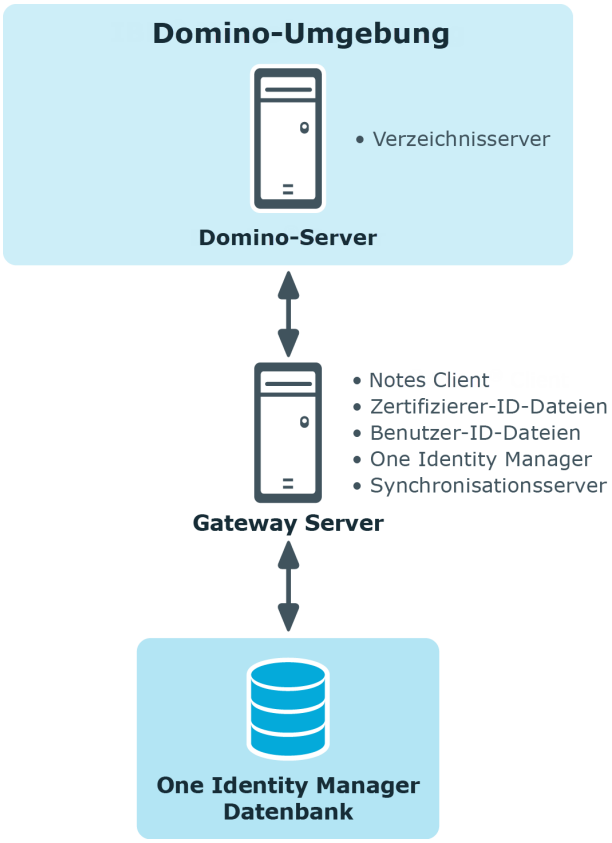
Innerhalb der One Identity Manager-Umgebung wird ein Server definiert, der alle administrativen Aufgaben, die Domino-Umgebung betreffend, ausführt. Dieser Server wird im Folgenden als Gateway Server bezeichnet. Der Gateway Server übernimmt die Funktion des Synchronisationsservers. Er ist selbst kein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

Vom Gateway Server werden alle Aktionen des Domino 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 Domino 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 Domino-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 Notes-Client-Kontext unter Verwendung der Notes 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 Domino Konnektors mit der Domino-Umgebung



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

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

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

Domino	One Identity Manager
Notes Zertifikat	Notes Zertifikat
Schablone	Notes Schablone
Richtlinie	Notes Richtlinie

One Identity Manager Benutzer für die Verwaltung einer Domino-Umgebung

In die Einrichtung und Verwaltung einer Domino-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 | Domino** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die

Benutzer	Aufgaben
	Zielsystemobjekte. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • 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.

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

Konfigurationsparameter für die Verwaltung von Domino-Umgebungen

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

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

Weitere Informationen finden Sie unter Konfigurationsparameter für die Verwaltung einer Domino-Umgebung auf Seite 246.

Synchronisieren einer Domino-Umgebung

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

- IBM Domino Server Version 8, 9 und 10
- HCL Domino Server Version 11 und 12
- IBM Notes Client Version 8.5.3 oder 10.0
- HCL Notes Client Version 11.0.1 und 12.0

  Die 64-Bit-Variante des Notes Client 12.0.1 wird derzeit nicht unterstützt.

HINWEIS: Da die Verwaltung der Objekte im One Identity Manager unabhängig von der Version der Zielsystemumgebung ist, wird auf das Zielsystem im One Identity Manager einheitlich mit der Bezeichnung Domino Bezug genommen.

Für den Abgleich der Informationen zwischen der One Identity Manager-Datenbank und der Domino-Umgebung sorgt der One Identity Manager Service.

Informieren Sie sich hier:

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

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

Detaillierte Informationen zum Thema

- Einrichten der Initialsynchronisation einer Domino-Umgebung auf Seite 17
- Anpassen der Synchronisationskonfiguration für Domino-Umgebungen auf Seite 35
- Ausführen einer Synchronisation auf Seite 50
- Fehleranalyse auf Seite 57

Einrichten der Initialsynchronisation einer Domino-Umgebung

Der Synchronization Editor stellt eine Projektvorlage bereit, mit der die Synchronisation von Notes Benutzerkonten und Gruppen eingerichtet werden kann. Nutzen Sie diese Projektvorlage, um Synchronisationsprojekte zu erstellen, mit denen Sie Daten aus einer Domino-Umgebung in Ihre One Identity Manager-Datenbank einlesen. Zusätzlich werden die notwendigen Prozesse angelegt, über die Änderungen an Zielsystemobjekten aus der One Identity Manager-Datenbank in das Zielsystem provisioniert werden.

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

1. Stellen Sie in der HCL Domino-Umgebung einen Benutzer für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Die One Identity Manager Bestandteile für die Verwaltung von Domino-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.

      HINWEIS: Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
    - Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.
3. Installieren und konfigurieren Sie den Gateway Server.
4. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.
5. Wenn durch den Domino Konnektor Benutzerkonten in der Domino-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 Domino-Umgebung auf Seite 18
- Systemanforderungen für den Gateway Servers auf Seite 21
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Notes Domäne auf Seite 28
- Allgemeine Stammdaten für Notes Zertifikate auf Seite 185
- Standardprojektvorlage für Domino auf Seite 249
- Konfigurationsparameter für die Verwaltung einer Domino-Umgebung auf Seite 246

Benutzer und Berechtigungen für die Synchronisation mit einer Domino-Umgebung

Bei der Synchronisation des One Identity Manager mit einer HCL Domino-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 Benutzerrechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Verzeichnisse und Dateien anlegen und bearbeiten. Das Benutzerkonto muss der Gruppe **Domänen-Benutzer** angehören. Das Benutzerkonto benötigt das erweiterte Benutzerrecht **Anmelden als Dienst**. Das Benutzerkonto benötigt Berechtigungen für den internen Webservice. HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so können Sie die Berechtigungen für den internen Webservice über folgenden Kommandozeilenaufruf vergeben: `netsh http add urlacl url=http://<IP-`

Benutzer	Berechtigungen
	`Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"` Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis. In der Standardinstallation wird der One Identity Manager installiert unter: • `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen) • `%ProgramFiles%\One Identity` (auf 64-Bit Betriebssystemen)
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 (Optional) Wenn Postfachdateien bereits während der Registrierung von Notes Benutzern erzeugt werden sollen, wird folgende Berechtigung benötigt, damit der Domino Konnektor lesend auf die erzeugten Postfachdateien zugreifen kann. • Übertragbare Berechtigung für den Synchronisationsbenutzer an der Schablone auf dem Domino-Server (`*.ntf`), die zum Erzeugen von Postfachdateien genutzt wird
Benutzer für den Zugriff auf	Um die Synchronisation über einen Anwendungsserver

Benutzer	Berechtigungen
die One Identity Manager-Datenbank	auszuführen, wird der Standard-Systembenutzer **Synchronization** bereitgestellt.

Verwandte Themen

- Postfachdateien erzeugen auf Seite 47

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.
- In der Datei `Notes.ini` setzen Sie `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 Domino-Umgebung.

Einrichten eines Gateway Servers

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.

Um den Gateway Server einzurichten

1. Konfigurieren Sie den Notes Client.
2. Installieren Sie den One Identity Manager Service mit dem Domino Konnektor und geben Sie den Gateway Server als Jobserver in der One Identity Manager-Datenbank bekannt.
3. (Optional) Um Benutzer-ID-Dateien über das ID-Restore-Verfahren wiederherstellen zu können, legen Sie eine Archivdatenbank zur Sicherung der ID-Dateien an.

Detaillierte Informationen zum Thema

- Systemanforderungen für den Gateway Servers auf Seite 21
- Notes Client konfigurieren auf Seite 22
- One Identity Manager Service auf dem Gateway Server installieren auf Seite 24
- Archivdatenbank zur Sicherung der Personendokumente anlegen auf Seite 27

Systemanforderungen für den Gateway Servers

Für die Einrichtung eines Gateway Servers muss ein Server bereitgestellt werden, auf dem die nachfolgend genannte Software installiert ist:

- Windows Betriebssystem

  Unterstützt werden die Versionen:

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

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.
- Windows Installer
- IBM Notes Client Version 8.5.3 oder 10.0 oder HCL Notes Client Version 11.0.1 oder 12.0

  HINWEIS:

  - Führen Sie die Installation im Einzelbenutzermodus aus.
  - Es muss eine echte Installation durchgeführt werden. Während der Installation werden Domino COM-Klassenbibliotheken registriert. Diese benötigt der Domino Konnektor.
- Schreibzugriff auf das Installationsverzeichnis des Notes Clients und auf das One Identity Manager Installationsverzeichnis.
- One Identity Manager Service, Domino 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 | Domino**.

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

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

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

Hinweise für die Synchronisation einer HCL Domino 12 Umgebung

Wenn die angebundene Domino-Umgebung Domino 12 nutzt und der Domino Konnektor schreibend auf das Zielsystem zugreift, dann muss auf dem Gateway Server die Notes Client Version 12 installiert sein. Die 64-Bit-Variante des Notes Client 12.0.1 wird derzeit nicht unterstützt.

Wenn nur lesend auf das Zielsystem zugegriffen wird, kann auf dem Gateway Server auch eine ältere Notes Client Version genutzt werden.

Notes Client konfigurieren

Um den Notes Client zu konfigurieren

1. Erweitern Sie die PATH-Variable um den Standardsuchpfad (Installationsverzeichnis) und das Datenverzeichnis (`<Installationsverzeichnis>\Data`).
    - Tragen Sie den Notes Installationspfad in den Standardsuchpfad des Betriebssystems (PATH-Variable) ein. Das ist der Pfad, in dem sich die `Notes.exe` befindet.
    - Fügen Sie den bei der Installation des 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 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 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 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

- Notes Zertifikate übernehmen auf Seite 23
- Kundenspezifische INI-Datei erstellen auf Seite 23

Notes Zertifikate übernehmen

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 Domino 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 Domino-Umgebung.

Kundenspezifische INI-Datei erstellen

Bei der Konfiguration des Notes Clients wird die Datei `Notes.ini` erzeugt. Diese Datei enthält verschiedene Konfigurationsinformationen, die der Domino Konnektor für den Zugriff auf das Zielsystem benötigt. Erstellen Sie eine Kopie dieser INI-Datei und stellen

Sie diese als kundenspezifische INI-Datei dem Domino 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.

One Identity Manager Service auf dem Gateway Server installieren

Auf dem Gateway Server muss der One Identity Manager Service mit dem Domino Konnektor installiert sein. Der Gateway Server muss im One Identity Manager als Jobserver bekannt sein.

Tabelle 5: Eigenschaften des Jobservers

Eigenschaft	Wert
Serverfunktion	Domino Konnektor
Maschinenrolle	Server | Jobserver | Domino

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: Das Programm führt eine Remote-Installation des One Identity Manager Service aus. Eine lokale Installation des Dienstes ist mit diesem Programm nicht möglich.

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*.

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*.

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

          Syntax:

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

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

4. Auf der Seite **Maschinenrollen** wählen Sie **Domino**.
5. Auf der Seite **Serverfunktionen** wählen Sie **Domino 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:
     1. Wählen Sie **Prozessabholung > sqlprovider**
     2. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     3. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
   - Für eine Verbindung zum Anwendungsserver:
     1. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
     2. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     3. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.
     4. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
     5. 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** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.
10. Wenn die Datenbank verschlüsselt ist, wählen Sie auf der Seite **Datenbankschlüsseldatei auswählen** die Datei mit dem privaten Schlüssel.
11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.

- **Computer**: Erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
- **Dienstkonto**: Erfassen Sie die Angaben zum Benutzerkonto unter dem der One Identity Manager Service läuft. Erfassen Sie das Benutzerkonto, das Kennwort zum Benutzerkonto und die Kennwortwiederholung.

Die Installation des Dienstes erfolgt mit dem Benutzerkonto, mit dem Sie an der administrativen Arbeitsstation angemeldet sind. Möchten Sie ein anderes Benutzerkonto für die Installation des Dienstes nutzen, können Sie dieses in den erweiterten Optionen eintragen. Angaben zum One Identity Manager Service können Sie ebenfalls über die erweiterten Optionen ändern, beispielsweise das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den One Identity Manager Service.

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.

Archivdatenbank zur Sicherung der Personendokumente anlegen

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 Benutzer-ID-Dateien über ID-Restore wiederherstellen auf Seite 161.

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

Tabelle 6: Benötigte Daten für die Kopie

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

Standardmäßig wird die Kopie des lokalen Adressbuchs für den angemeldeten Benutzer verschlüsselt. Damit der Domino 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 Domino-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 Domino-Umgebung einzurichten. Nachfolgend sind die Schritte für die initiale Einrichtung eines Synchronisationsprojektes beschrieben. Ausführliche Informationen zur Einrichtung der Synchronisation finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

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

Benötigte Informationen für die Erstellung eines Notes Synchronisationsprojektes

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

Tabelle 7: 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 Kundenspezifische INI-Datei erstellen auf Seite 23.

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 Domino 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 Domino-Umgebung auf Seite 18.
Synchronisationsserver für die Notes Domäne	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 Domino Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften. **Tabelle 8: Zusätzliche Eigenschaften für den Jobserver** **Eigenschaft** / **Wert** Serverfunktion / Domino Konnektor Maschinenrolle / Server/Jobserver/Domino Weitere Informationen finden Sie unter One Identity Manager Service auf dem Gateway Server installieren auf Seite 24.
Verbindungsdaten zur One Identity Manager-Datenbank	• Datenbankserver • Name der Datenbank • SQL Server Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung verwendet wird Die Verwendung der integrierten Windows-Authentifizierung wird nicht empfohlen. Sollten Sie das Verfahren dennoch einsetzen, stellen Sie sicher,

Angaben	Erläuterungen
	dass Ihre Umgebung Windows-Authentifizierung unterstützt.
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 • Domino 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*.

Initiales Synchronisationsprojekt für eine Notes Domäne erstellen

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

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

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

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

Um ein initiales Synchronisationsprojekt für eine Notes Domäne einzurichten

1. Starten Sie das Launchpad auf 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 Domino** 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 Domino Verzeichnis** erfassen Sie die Verbindungsparameter, die der Domino Konnektor zur Anmeldung am Zielsystem benötigt.

   Tabelle 9: Verbindungsdaten zum Domino-Server

Eigenschaft	Beschreibung
INI-Datei	Name und Pfad zur kundenspezifischen INI-Datei.

Eigenschaft	Beschreibung
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 Domino 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 10: Zielsystemzugriff festlegen

Option	Bedeutung
Das Zielsystem soll nur eingelesen werden.	Gibt an, ob nur ein Synchronisationsworkflow zum initialen Einlesen des Zielsystems in die One Identity

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

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

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

    a. Klicken Sie , um einen neuen Jobserver anzulegen.

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

    c. Klicken Sie **OK**.

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

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

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

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

Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

HINWEIS:

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

  Bevor Sie das Synchronisationsprojekt nutzen, prüfen Sie die Fehler. In der Ansicht **Allgemein** auf der Startseite des Synchronization Editor klicken Sie dafür **Projekt prüfen**.
- Wenn das Synchronisationsprojekt nicht sofort aktiviert werden soll, deaktivieren Sie die Option **Synchronisationsprojekt speichern und sofort aktivieren**. In diesem Fall speichern Sie das Synchronisationsprojekt manuell vor dem Beenden des Synchronization Editor.
- Die Verbindungsdaten zum Zielsystem werden in einem Variablenset gespeichert und können bei Bedarf im Synchronization Editor in der Kategorie **Konfiguration > Variablen** angepasst werden.

Verwandte Themen

- Synchronisationsprotokoll konfigurieren auf Seite 34
- Anpassen der Synchronisationskonfiguration für Domino-Umgebungen auf Seite 35
- Standardprojektvorlage für Domino auf Seite 249

Synchronisationsprotokoll konfigurieren

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

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

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

   - ODER -

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

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

5. Klicken Sie **OK**.

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

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

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 51

Anpassen der Synchronisationskonfiguration für Domino-Umgebungen

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 Domino-Umgebung provisioniert.

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

- Um bei der Synchronisation den One Identity Manager als primäres System zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um festzulegen, welche 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.
- Um zusätzliche Schemaeigenschaften zu synchronisieren, aktualisieren Sie das Schema im Synchronisationsprojekt. Nehmen Sie die Schemaerweiterungen in das Mapping auf.

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

Detaillierte Informationen zum Thema

- Synchronisation in die Domino-Umgebung konfigurieren auf Seite 36
- Synchronisation verschiedener Notes Domänen konfigurieren auf Seite 37
- Schema aktualisieren auf Seite 40
- Einstellungen der Systemverbindung zur Notes Domäne ändern auf Seite 37

Synchronisation in die Domino-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 primäres System zu nutzen, benötigen Sie zusätzlich einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.

Um eine Synchronisationskonfiguration für die Synchronisation in die Domino-Umgebung zu erstellen

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

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

Verwandte Themen

- Synchronisation verschiedener Notes Domänen konfigurieren auf Seite 37

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.
- Die Verbindungsparameter zum Zielsystem sind als Variablen hinterlegt.

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 im Synchronization Editor das Synchronisationsprojekt.
3. Erstellen Sie für jede weitere Domäne ein neues Basisobjekt.
    - Verwenden Sie den Assistenten zur Anlage eines Basisobjektes.
    - Wählen Sie im Assistenten den Domino Konnektor.
    - Geben Sie die Verbindungsparameter bekannt. Die Verbindungsparameter werden in einem spezialisierten Variablenset gespeichert.

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

Verwandte Themen

- Synchronisation in die Domino-Umgebung konfigurieren auf Seite 36

Einstellungen der Systemverbindung zur Notes Domäne ändern

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

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

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

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

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

Detaillierte Informationen zum Thema

- Verbindungsparameter im Variablenset bearbeiten auf Seite 38
- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 39

Verbindungsparameter im Variablenset bearbeiten

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

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

Um die Verbindungsparameter in einem spezialisierten Variablenset anzupassen

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

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

   Im unteren Bereich der Dokumentenansicht werden alle spezialisierten Variablensets angezeigt.

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

    - ODER -

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

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

Verwandte Themen

- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 39

Eigenschaften der Zielsystemverbindung bearbeiten

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

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

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

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

Um die Verbindungsparameter mit dem Systemverbindungsassistenten zu bearbeiten

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

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

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

Verwandte Themen

- Verbindungsparameter im Variablenset bearbeiten auf Seite 38

Schema aktualisieren

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

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

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

- ein Schema geändert wurde, durch:
  - Änderungen am Zielsystemschema
  - unternehmensspezifische Anpassungen des One Identity Manager Schemas
  - eine Update-Migration des One Identity Manager
- ein Schema im Synchronisationsprojekt komprimiert wurde, durch:

- die Aktivierung des Synchronisationsprojekts
- erstmaliges Speichern des Synchronisationsprojekts
- Komprimieren eines Schemas

Um das Schema einer Systemverbindung zu aktualisieren

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

   - ODER -

   Wählen Sie die Kategorie **Konfiguration > One Identity Manager Verbindung**.
3. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Die Schemadaten werden neu geladen.

Um ein Mapping zu bearbeiten

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

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

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

Beschleunigung der Synchronisation durch Revisionsfilterung

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.

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

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

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

Provisionierung von Mitgliedschaften konfigurieren

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

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

  Beispiel: Liste von Benutzerkonten in der Eigenschaft `Members` einer Notes Gruppe (`Group`)
- 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 **HCL Domino > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Domino**.
3. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
4. Wählen Sie die Zuordnungstabellen, für die Sie die Einzelprovisionierung ermöglichen möchten. Mehrfachauswahl ist möglich.
5. Klicken Sie **Merge-Modus**.

   HINWEIS:

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

     Beispiel: `NDOGroupInGroup`, `NDOMailInDBInGroup`, `NDOServerInGroup` und `NDOUSerInGroup`
6. Speichern Sie die Änderungen.

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

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

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

Um die originale Bedingung wiederherzustellen

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

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

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

Beispiel für eine Bedingung an der Zuordnungstabelle `NDOUserInGroup`:

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

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

Einzelobjektsynchronisation konfigurieren

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

Voraussetzungen

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

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

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

1. Wählen Sie im Manager die Kategorie **HCL Domino > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Domino**.
3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.

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

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

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

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 53
- Ausstehende Objekte nachbearbeiten auf Seite 54

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 Domino-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.
   - Für Jobserver, die an der Lastverteilung teilnehmen, muss die Option **Keine Prozesszuteilung** deaktiviert sein.
   - Weisen Sie diesen Jobservern die Serverfunktion **Domino 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

- Jobserver für Domino-spezifische Prozessverarbeitung auf Seite 237

Benutzertyp festlegen

Neue Benutzer werden in der Domino-Umgebung standardmäßig als **Full Client User** registriert. Welcher Benutzertyp für die Registrierung genutzt wird, ist in der Synchronisationsvariable **UserType** festgelegt. Mögliche Werte sind:

- **174**: LIMITED CLIENT USER
- **175**: DESKTOP CLIENT USER
- **176**: FULL CLIENT USER

Um den Standardbenutzertyp zu ändern

- Bearbeiten Sie im Synchronisationsprojekt die Variable **UserType** und erfassen Sie den gewünschten Wert.

  Um eine Variable zu bearbeiten

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

3. Wählen Sie die Variable und bearbeiten Sie deren Wert.
4. Speichern Sie die Änderungen.

Ausführliche Informationen zu Variablen und Variablensets finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Verbindungsparameter im Variablenset bearbeiten auf Seite 38

Postfachdateien erzeugen

Ob und auf welchem Weg in der Domino-Umgebung Postfachdateien erzeugt werden, ist abhängig von den Angaben am Benutzerkonto und von den Einstellungen der Konfigurationsparameter.

Voraussetzungen

- Am Benutzerkonto sind Pfad und Dateiname der Postfachdatei angegeben.

  Fehlt diese Angabe, wird keine Postfachdatei erzeugt.
- Im Konfigurationsparameter **TargetSystem | NDO | MailFilePath** ist das Verzeichnis angegeben, auf dem die Postfachdateien auf dem Mailserver abgelegt werden.

Zugriffsstufe konfigurieren

Standardmäßig wird für den Besitzer der Postfachdatei die Zugriffsstufe **Manager** gesetzt.

Um eine andere Zugriffsstufe zu setzen

- Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | NDO | Accounts | MailFileAccessRole** und wählen Sie als Wert die Zugriffsstufe, die alle neuen Postfachdateien erhalten sollen. Mögliche Wert sind **Manager**, **Editor**, **Designer**.

Postfachdatei erzeugen

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.

Die Postfachdatei kann auch bereits während der Registrierung des Notes Benutzers erzeugt werden. In diesem Fall wird die Schablone des Notes Servers verwendet, auf dem der Benutzer registriert wird.

Um die Postfachdatei während der Registrierung zu erzeugen

- Bearbeiten Sie die Variable **UserCreateMailDb** im Synchronisationsprojekt. Erfassen Sie den Wert **1**.

  Um eine Variable zu bearbeiten

  1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
  2. Wählen Sie die Kategorie **Konfiguration > Variablen**.
  3. Wählen Sie die Variable und bearbeiten Sie deren Wert.
  4. Speichern Sie die Änderungen.

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.

Stellen Sie sicher, dass auf die Schablone der Postfachdatei auf dem Domino-Server eine übertragbare Berechtigung für den Synchronisationsbenutzer gesetzt ist, damit der Domino Konnektor lesend auf die erzeugten Postfachdateien zugreifen kann.

Verwandte Themen

- E-Mail-System von Notes Benutzerkonten auf Seite 145
- Zusätzliche Stammdaten von Notes Benutzerkonten auf Seite 147
- Verbindungsparameter im Variablenset bearbeiten auf Seite 38

Benutzer-ID-Dateien erzeugen und speichern

Beim Anlegen eines Benutzers im Zielsystem wird die Benutzer-ID-Datei zur Authentifizierung des Benutzers erzeugt. Der Domino Konnektor benötigt Informationen über die minimale Kennwortlänge, die Verschlüsselungsstärke und über den Speicherort der ID-Dateien. Beim Erzeugen der ID-Dateien werden die Einstellungen in folgenden Synchronisationsvariablen berücksichtigt.

Tabelle 11: Einstellungen für neue Benutzer-ID-Dateien

Variable	Beschreibung
UserIsNorthAmerican	Gibt an, ob neu erzeugte ID-Dateien kompatibel zur US-amerikanischen und kanadischen Domino Version sind. Wert **1**: Alle neu erzeugten Benutzer-ID-Dateien werden mit nordamerikanischer Verschlüsselungsstärke berechnet. Standard: **0**

Variable	Beschreibung
UserMinPwdLen	Gibt die minimalen Kennwortlänge an, die in allen neu zu berechnenden Benutzer-ID-Dateien zu setzen ist. Standard: **0**
UserStoreIDInAddressbook	Gibt an, ob die erstellte ID-Datei als Attachment an das Personendokument angehängt oder auf dem Gateway Server gespeichert wird. Standard: **0** - Die ID-Datei wird als Attachment an das Personendokument angehängt.

Um eine Variable zu bearbeiten

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Variablen**.
3. Wählen Sie die Variable und bearbeiten Sie deren Wert.
4. Speichern Sie die Änderungen.

Ausführliche Informationen zu Variablen und Variablensets finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Um die Benutzer-ID-Dateien auf dem Gateway Server zu speichern

1. Bearbeiten Sie im Synchronisationsprojekt die Variable **UserStoreIDInAddressbook**. Erfassen Sie den Wert **1**.
2. Bearbeiten Sie im Manager die Stammdaten der Domäne und geben Sie den **Pfad der Benutzer-ID-Dateien** an. Erfassen Sie den Pfad, unter dem die Dateien gespeichert werden sollen.

   Wenn an der Domäne kein Standardpfad angegeben ist, können Sie den Pfad an den Mailservern der Benutzerkonten hinterlegen. Wenn der Pfad weder an der Domäne noch am Mailserver angegeben ist, nutzt der Domino Konnektor den Standardpfad, der an der Variable **UserIDFilesDefaultPath** im Synchronisationsprojekt hinterlegt ist.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Notes Domänen auf Seite 135
- Allgemeine Stammdaten von Notes Servern auf Seite 203
- E-Mail-System von Notes Benutzerkonten auf Seite 145
- Verbindungsparameter im Variablenset bearbeiten auf Seite 38

Ausführen einer Synchronisation

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

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

Detaillierte Informationen zum Thema

- Synchronisationen starten auf Seite 50
- Synchronisation deaktivieren auf Seite 52
- Synchronisationsergebnisse anzeigen auf Seite 51
- Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) auf Seite 59

Synchronisationen starten

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

Um regelmäßige Synchronisationen auszuführen

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

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

Um die initiale Synchronisation manuell zu starten

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

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

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

Synchronisationsergebnisse anzeigen

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

Um das Protokoll einer Synchronisation anzuzeigen

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

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

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

Um das Protokoll einer Provisionierung anzuzeigen

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

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

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

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

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

Verwandte Themen

- Synchronisationsprotokoll konfigurieren auf Seite 34
-

Synchronisation deaktivieren

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

Um regelmäßige Synchronisationen zu verhindern

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

   Synchronisationen können nun nur noch manuell gestartet werden.

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

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

Um das Synchronisationsprojekt zu deaktivieren

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

Verwandte Themen

- Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) auf Seite 59

Einzelobjekte synchronisieren

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

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

Um ein Einzelobjekt zu synchronisieren

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

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

Besonderheiten bei der Synchronisation von Mitgliederlisten

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

Beispiel:

Basisobjekt für die Zuweisung von Benutzerkonten an Gruppen ist die Gruppe.

Im Zielsystem wurde ein Benutzerkonto an eine Gruppe zugewiesen. Um diese Zuweisung zu synchronisieren, wählen Sie im Manager die Gruppe, der das

Benutzerkonto zugewiesen wurde, und führen Sie die Einzelobjektsynchronisation aus. Dabei werden alle Mitgliedschaften für diese Gruppe synchronisiert.

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

Detaillierte Informationen zum Thema

- Einzelobjektsynchronisation konfigurieren auf Seite 44

Aufgaben nach einer Synchronisation

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

- Ausstehende Objekte nachbearbeiten auf Seite 54
- Notes Benutzerkonten über Kontendefinitionen verwalten auf Seite 57

Ausstehende Objekte nachbearbeiten

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

Ausstehende Objekte

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

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

Führen Sie dafür einen Zielsystemabgleich durch.

Um ausstehende Objekte nachzubearbeiten

1. Wählen Sie im Manager die Kategorie **HCL Domino > Zielsystemabgleich: Domino**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp **Domino** als Synchronisationstabellen zugewiesen sind.

2. Öffnen Sie auf dem Formular **Zielsystemabgleich**, in der Spalte **Tabelle/Objekt** den Knoten der Tabelle, für die sie ausstehende Objekte nachbearbeiten möchten.

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

   - Das Synchronisationsprotokoll wurde bereits gelöscht.

     - ODER -

   - Im Zielsystem wurde eine Zuweisung aus einer Mitgliederliste gelöscht.

     Bei der Synchronisation wird das Basisobjekt der Zuordnung aktualisiert. Dafür erscheint ein Eintrag im Synchronisationsprotokoll. Der Eintrag in der Zuordnungstabelle wird als ausstehend markiert, es gibt jedoch keinen Eintrag im Synchronisationsprotokoll.

   - Im Zielsystem wurde ein Objekt gelöscht, das eine Mitgliederliste enthält.

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

   TIPP:

   Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

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

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

Tabelle 12: Methoden zur Behandlung ausstehender Objekte

Symbol	Methode	Beschreibung
	Löschen	Das Objekt wird sofort in der One Identity Manager-Datenbank gelöscht. Eine Löschverzögerung wird nicht berücksichtigt. Indirekte Mitgliedschaften können nicht gelöscht werden.
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung **Ausstehend** wird für das Objekt entfernt. Es wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt.

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 das Symbol .

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

Verwandte Themen

- Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen auf Seite 56

Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen

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

Um kundenspezifische Tabellen in den Zielsystemabgleich aufzunehmen

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

3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die kundenspezifischen Tabellen zu, für die Sie ausstehende Objekte behandeln möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die kundenspezifischen Tabellen, für die ausstehende Objekte in das Zielsystem publiziert werden dürfen und aktivieren Sie die Option **Publizierbar**.
8. Speichern Sie die Änderungen.

Verwandte Themen

- Ausstehende Objekte nachbearbeiten auf Seite 54

Notes Benutzerkonten über Kontendefinitionen verwalten

Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Personen erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für die 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.

Detaillierte Informationen zum Thema

- Kontendefinitionen an verbundene Benutzerkonten zuweisen auf Seite 89

Fehleranalyse

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

- Synchronisation simulieren

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

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

- Meldungen protokollieren

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

- Startinformation zurücksetzen

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

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

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 51

Datenfehler bei der Synchronisation ignorieren

Standardmäßig werden Objekte mit fehlerhaften Daten nicht synchronisiert. Diese Objekte können synchronisiert werden, sobald die fehlerhaften Daten korrigiert wurden. In einzelnen Situationen kann es notwendig sein, solche Objekte dennoch zu synchronisieren und nur die fehlerhaften Objekteigenschaften zu ignorieren. Dieses Verhalten kann für die Synchronisation in den One Identity Manager konfiguriert werden.

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

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

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

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

   Fehler in Standardspalten, wie Primärschlüssel oder UID-Spalten, und

Pflichteingabespalten können nicht ignoriert werden.

5. Speichern Sie die Änderungen.

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

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

Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus)

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

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

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

Voraussetzungen

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

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

Um den Offline-Modus für ein Basisobjekt zuzulassen

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

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

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

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

Um ein Zielsystem als offline zu kennzeichnen

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

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

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

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

Verwandte Themen

- Synchronisation deaktivieren auf Seite 52

Managen von Notes Benutzerkonten und Personen

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

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

- Personen erhalten ihre Benutzerkonten automatisch über Kontendefinitionen.

  Hat eine Person noch kein Benutzerkonto in einer 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.

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

Verwandte Themen

- Kontendefinitionen für Notes Benutzerkonten auf Seite 62
- Automatische Zuordnung von Personen zu Notes Benutzerkonten auf Seite 83
- Notes Benutzerkonten erstellen und bearbeiten auf Seite 139

Kontendefinitionen für Notes Benutzerkonten

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

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

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

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

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

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

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

Detaillierte Informationen zum Thema

- Notes Kontendefinitionen erstellen auf Seite 63
- Notes Kontendefinitionen bearbeiten auf Seite 64
- Stammdaten von Notes Kontendefinitionen auf Seite 64
- Automatisierungsgrade bearbeiten auf Seite 67
- Automatisierungsgrade erstellen auf Seite 68
- Stammdaten von Automatisierungsgraden auf Seite 69
- Abbildungsvorschriften für IT Betriebsdaten erstellen auf Seite 70
- IT Betriebsdaten erfassen auf Seite 72
- IT Betriebsdaten ändern auf Seite 73
- Zuweisen der Notes Kontendefinition an Personen auf Seite 74
- Notes Kontendefinitionen an Zielsysteme zuweisen auf Seite 80
- Notes Kontendefinitionen löschen auf Seite 81

Notes Kontendefinitionen erstellen

Um eine Kontendefinition zu erstellen

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

Verwandte Themen

- Stammdaten von Notes Kontendefinitionen auf Seite 64
- Notes Kontendefinitionen bearbeiten auf Seite 64

Notes Kontendefinitionen bearbeiten

Um eine Kontendefinition zu bearbeiten

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

Verwandte Themen

- Stammdaten von Notes Kontendefinitionen auf Seite 64
- Notes Kontendefinitionen erstellen auf Seite 63

Stammdaten von Notes Kontendefinitionen

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 13: 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	Angabe der vorausgesetzten Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch zugeordnet. Für eine HCL Domino 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. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER |**

Eigenschaft	Beschreibung
	CalculateRiskIndex aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Leistungsposition	Leistungsposition, über welche die Kontendefinition im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.
IT Shop	Gibt an, ob die Kontendefinition über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Personen und Rollen außerhalb des IT Shop zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig.
Automatische Zuweisung zu Personen	Gibt an, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Um die Kontendefinition automatisch an alle internen Personen zuzuweisen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Personen aktivieren**. Die Kontendefinition wird an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine neue interne Person erstellt wird, erhält diese Person ebenfalls automatisch diese Kontendefinition. Um die automatische Zuweisung der Kontendefinition von allen Personen zu entfernen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Personen deaktivieren**. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.
Kontendefinition bei 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: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.

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

Automatisierungsgrade bearbeiten

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

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

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

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

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

- Um die Berechtigungen zu entziehen, wenn eine Person deaktiviert, gelöscht oder als sicherheitsgefährdend eingestuft wird, können die Benutzerkonten der Person gesperrt werden. Wird die Person zu einem späteren Zeitpunkt wieder aktiviert, werden ihre Benutzerkonten ebenfalls wieder freigeschaltet.
- Zusätzlich kann die Vererbung der Gruppenmitgliedschaften definiert werden. Die Unterbrechung der Vererbung kann beispielsweise gewünscht sein, wenn die Benutzerkonten einer Person gesperrt sind und somit auch nicht in Gruppen Mitglied sein dürfen. Während dieser Zeit sollen keine Vererbungsvorgänge für diese Personen berechnet werden. Bestehende Gruppenmitgliedschaften werden dann gelöscht!

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie im Manager die Kategorie **HCL Domino > Basisdaten zur Konfiguration > Kontendefinitionen > Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad.

3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Automatisierungsgrades.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von Automatisierungsgraden auf Seite 69
- Automatisierungsgrade erstellen auf Seite 68
- Automatisierungsgrade an Notes Kontendefinitionen zuweisen auf Seite 68

Automatisierungsgrade erstellen

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

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

Um einen Automatisierungsgrad zu erstellen

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

Verwandte Themen

- Stammdaten von Automatisierungsgraden auf Seite 69
- Automatisierungsgrade bearbeiten auf Seite 67

Automatisierungsgrade an Notes Kontendefinitionen zuweisen

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

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

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

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

   Um eine Zuweisung zu entfernen

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

Stammdaten von Automatisierungsgraden

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 14: Stammdaten eines Automatisierungsgrades

Eigenschaft	Beschreibung
Automatisierungsgrad	Bezeichnung des Automatisierungsgrades.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Betriebsdaten überschreibend	Gibt an, ob Daten an Benutzerkonten, die sich aus den IT Betriebsdaten bilden, automatisch aktualisiert werden. Zulässige Werte sind: • **Niemals**: Die Daten werden nicht aktualisiert. (Standard) • **Immer**: Die Daten werden immer aktualisiert. • **Nur initial**: Die Daten werden nur initial ermittelt.
Gruppen bei zeitweiliger Deaktivierung beibehalten	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei zeitweiliger Deaktivierung sperren	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Personen gesperrt werden sollen.
Gruppen bei dauerhafter Deaktivierung beibehalten	Gibt an, ob die Benutzerkonten dauerhaft deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.

Eigenschaft	Beschreibung
Benutzerkonten bei dauerhafter Deaktivierung sperren	Gibt an, ob die Benutzerkonten dauerhaft deaktivierter Personen gesperrt werden sollen.
Gruppen bei verzögertem Löschen beibehalten	Gibt an, ob die Benutzerkonten zum Löschen markierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei verzögertem Löschen sperren	Gibt an, ob die Benutzerkonten zum Löschen markierter Personen gesperrt werden sollen.
Gruppen bei Sicherheitsgefährdung beibehalten	Gibt an, ob die Benutzerkonten von sicherheitsgefährdenden Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei Sicherheitsgefährdung sperren	Gibt an, ob die Benutzerkonten von sicherheitsgefährdenden Personen gesperrt werden sollen.
Gruppen bei deaktiviertem Benutzerkonto beibehalten	Gibt an, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen.

Abbildungsvorschriften für IT Betriebsdaten erstellen

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

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

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

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

          Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option **Immer Standardwert verwenden** setzen.
    - **Standardwert**: Standardwert der Eigenschaft für das Benutzerkonto einer Person, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann.
    - **Immer Standardwert verwenden**: Gibt an, ob die Eigenschaft des Benutzerkontos immer mit dem Standardwert besetzt wird. Es erfolgt keine dynamische Ermittlung der IT Betriebsdaten aus einer Rolle.
    - **Benachrichtigung bei Verwendung des Standards**: Gibt an, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkontos mit Standardwerten** verwendet.

      Um die Mailvorlage zu ändern, passen Sie im Designer den Konfigurationsparameter **TargetSystem | NDO | Accounts | MailTemplateDefaultValues** an.
5. Speichern Sie die Änderungen.

Verwandte Themen

- IT Betriebsdaten erfassen auf Seite 72

IT Betriebsdaten erfassen

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

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

Beispiel:

In der Regel erhält jede Person der Abteilung A ein Standardbenutzerkonto in der 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.
    - **Wirksam für**: Legen Sie den Anwendungsbereich der IT Betriebsdaten fest. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden.

Um den Anwendungsbereich festzulegen

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

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

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

d. Klicken Sie **OK**.

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

  In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

- **Wert**: Erfassen Sie den konkreten Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Abbildungsvorschriften für IT Betriebsdaten erstellen auf Seite 70

IT Betriebsdaten ändern

Sobald sich die IT Betriebsdaten ändern, müssen Sie diese Änderungen für bestehende Benutzerkonten übernehmen. Dafür führen Sie die Bildungsregeln an den betroffenen Spalten erneut aus. Bevor Sie die Bildungsregeln ausführen, prüfen Sie, welche Auswirkungen eine Änderung der IT Betriebsdaten auf bestehende Benutzerkonten hat. Für jede betroffene Spalte an jedem betroffenen Benutzerkonto können Sie entscheiden, ob die Änderung in die One Identity Manager-Datenbank übernommen werden soll.

Voraussetzungen

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

  - ODER -

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

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

Um die Bildungsregeln auszuführen

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

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

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

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Notes 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.

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

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

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

Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

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

   - ODER -

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

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

Notes Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

Notes Kontendefinitionen an Geschäftsrollen zuweisen

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

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

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

    Um eine Zuweisung zu entfernen
    - Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Notes Kontendefinitionen an alle Personen zuweisen

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

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

Um eine Kontendefinition an alle Personen zuzuweisen

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

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

Notes Kontendefinitionen direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

Notes Kontendefinitionen an Systemrollen zuweisen

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

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

Um Kontendefinitionen in eine Systemrolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

Notes Kontendefinitionen in den IT Shop aufnehmen

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

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

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Kontendefinition im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.
- Soll die Kontendefinition nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss sie zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen ist dann nicht mehr zulässig.

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

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

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontendefinition an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

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

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

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

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

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

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

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

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

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

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

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

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

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

Verwandte Themen

- Stammdaten von Notes Kontendefinitionen auf Seite 64
- Notes Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 75
- Notes Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 76
- Notes Kontendefinitionen direkt an Personen zuweisen auf Seite 77
- Notes Kontendefinitionen an Systemrollen zuweisen auf Seite 77

Notes Kontendefinitionen an Zielsysteme zuweisen

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

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

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

Um die Kontendefinition an ein Zielsystem zuzuweisen

1. Wählen Sie im Manager in der Kategorie **HCL Domino > 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.

Verwandte Themen

- Automatische Zuordnung von Personen zu Notes Benutzerkonten auf Seite 83

Notes Kontendefinitionen löschen

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

Um eine Kontendefinition zu löschen

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

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

   e. Speichern Sie die Änderungen.

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

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

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

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

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

   e. Klicken Sie **OK**.

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

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

   a. Wählen Sie im Manager die Kategorie **HCL Domino > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

   e. Klicken Sie **OK**.

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

6. Entfernen Sie die Zuordnung der Kontendefinition als vorausgesetzte Kontendefinition einer anderen Kontendefinition. Solange die Kontendefinition Voraussetzung einer anderen Kontendefinition ist, kann sie nicht gelöscht werden. Prüfen Sie alle Kontendefinitionen.
    a. Wählen Sie im Manager die Kategorie **HCL Domino > 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 **HCL Domino > 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 **HCL Domino > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Klicken Sie , um die Kontendefinition zu löschen.

Automatische Zuordnung von Personen zu Notes Benutzerkonten

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

Für die automatische Personenzuordnung definieren Sie Kriterien für die Ermittlung der Personen. Wird durch den eingesetzten Modus ein Benutzerkonto mit einer Person verbunden, so erhält das Benutzerkonto durch interne Verarbeitung den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des

Benutzerkontos eingetragen ist. Abhängig davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden.

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

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

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

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

- Wenn Personen bei der Synchronisation von Benutzerkonten zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | 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
  ```

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

  Um die Ausschlussliste für die automatische Personenzuordnung zu bearbeiten

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

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

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

Jeder Eintrag in der Liste wird als Teil eines regulären Ausdrucks behandelt. Metazeichen für reguläre Ausdrücke können verwendet werden.

5. Um einen Eintrag zu löschen, wählen Sie den Eintrag und klicken Sie **Löschen**.
6. Klicken Sie **OK**.

- Legen Sie über den Konfigurationsparameter **TargetSystem | 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.

Weitere Informationen finden Sie unter Notes Benutzerkonten über Kontendefinitionen verwalten auf Seite 57.

Verwandte Themen

- Notes Kontendefinitionen erstellen auf Seite 63
- Notes Kontendefinitionen an Zielsysteme zuweisen auf Seite 80
- Automatisierungsgrad an Notes Benutzerkonten ändern auf Seite 89
- Suchkriterien für die automatische Personenzuordnung bearbeiten auf Seite 86

Suchkriterien für die automatische Personenzuordnung bearbeiten

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

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

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

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

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

Um Kriterien für die Personenzuordnung festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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 15: 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.

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

Verwandte Themen

- Automatische Zuordnung von Personen zu Notes Benutzerkonten auf Seite 83
- Personen suchen und direkt an Benutzerkonten zuordnen auf Seite 87

Personen suchen und direkt an Benutzerkonten zuordnen

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

Tabelle 16: Ansichten zur manuellen Zuordnung

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

Um Suchkriterien auf die Benutzerkonten anzuwenden

1. Wählen Sie im Manager die Kategorie **HCL Domino > Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.
3. Wählen Sie die Aufgabe **Suchkriterien für die Personenzuordnung definieren**.
4. Im unteren Bereich des Formulars klicken Sie **Neu laden**.

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

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

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

Um Personen direkt über die Vorschlagsliste zuzuordnen

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

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

  - ODER -

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

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

Um Zuordnungen zu entfernen

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

       Von den ausgewählten Benutzerkonten werden die zugeordneten Personen entfernt.

Automatisierungsgrad an Notes Benutzerkonten ändern

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

Um den Automatisierungsgrad für ein Benutzerkonto zu ändern

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

Verwandte Themen

- Allgemeine Stammdaten für Notes Benutzerkonten auf Seite 141

Kontendefinitionen an verbundene Benutzerkonten zuweisen

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

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

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 **HCL Domino > 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

- Kontendefinitionen für Notes Benutzerkonten auf Seite 62
- Notes Kontendefinitionen an Zielsysteme zuweisen auf Seite 80

Personen manuell mit Notes Benutzerkonten verbinden

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

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

Um einer Person manuell Benutzerkonten zuzuweisen

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

Verwandte Themen

- Unterstützte Typen von Benutzerkonten auf Seite 90

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 17: Identitäten von Benutzerkonten

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

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

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

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

  Benutzerkonten mit einer Zusatzidentität, einer Gruppenidentität oder einer Dienstidentität verbinden Sie mit Pseudo-Personen, die keinen Bezug zu einer realen

Person haben. Diese Pseudo-Personen werden benötigt, um Berechtigungen an die Benutzerkonten vererben zu können. Bei der Auswertung von Berichten, Attestierungen oder Complianceprüfungen prüfen Sie, ob die Pseudo-Personen gesondert betrachtet werden müssen.

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

- Privilegiertes Benutzerkonto

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

Detaillierte Informationen zum Thema

- Standardbenutzerkonten auf Seite 92
- Administrative Benutzerkonten auf Seite 93
- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 94
- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 95
- Privilegierte Benutzerkonten auf Seite 96

Standardbenutzerkonten

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

Um Standardbenutzerkonten über Kontendefinitionen zu erstellen

1. Erstellen Sie eine Kontendefinition und weisen Sie die Automatisierungsgrade **Unmanaged** und **Full managed** zu.
2. Legen Sie für jeden Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll.
3. Erstellen Sie eine Abbildungsvorschrift für die IT Betriebsdaten.

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

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

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

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

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

5. Weisen Sie die Kontendefinition an die Personen zu.

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

Verwandte Themen

- Kontendefinitionen für Notes Benutzerkonten auf Seite 62

Administrative Benutzerkonten

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

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

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

Verwandte Themen

- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 94
- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 95

Administrative Benutzerkonten für eine Person bereitstellen

Voraussetzungen

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

Um ein administratives Benutzerkonto für eine Person bereitzustellen

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

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

Verwandte Themen

- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 95
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Administrative Benutzerkonten für mehrere Personen bereitstellen

Voraussetzung

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

Um ein administratives Benutzerkonto für mehrere Personen bereitzustellen

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

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

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

    Um eine Zuweisung zu entfernen

    - Wählen Sie die Person und doppelklicken Sie .

Verwandte Themen

- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 94
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Privilegierte Benutzerkonten

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

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

Um privilegierte Benutzerkonten über Kontendefinitionen zu erstellen

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

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

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

   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IsPrivilegedAccount` den Standardwert **1** und aktivieren Sie die Option **Immer Standardwert verwenden**.
   - Zusätzlich können Sie eine Abbildungsvorschrift für die Spalte `IdentityType` festlegen. Die Spalte besitzt verschiedene zulässige Werte, die privilegierte

Benutzerkonten repräsentieren.

- Um zu verhindern, das privilegierte Benutzerkonten die Berechtigungen des Standardbenutzers erben, definieren Sie eine Abbildungsvorschrift für die Spalte `IsGroupAccount` mit dem Standardwert **0** und aktivieren Sie die Option **Immer Standardwert verwenden**.

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

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

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

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

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

Verwandte Themen

- Kontendefinitionen für Notes Benutzerkonten auf Seite 62

Löschverzögerung für Notes Benutzerkonten festlegen

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

Sie haben die folgenden Möglichkeiten die Löschverzögerung zu konfigurieren.

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

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

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

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

Beispiel:

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

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

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

Managen von Mitgliedschaften in Notes Gruppen

In Notes Benutzerkonten können in Notes Gruppen zusammengefasst werden. Über die Notes Gruppen wird der Zugriff auf Ressourcen der Domino-Umgebung geregelt.

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

Detaillierte Informationen zum Thema

- Zuweisen von Notes Gruppen an Notes Benutzerkonten auf Seite 99
- Wirksamkeit von Mitgliedschaften in Notes Gruppen auf Seite 109
- Vererbung von Notes Gruppen anhand von Kategorien auf Seite 111
- Übersicht aller Zuweisungen auf Seite 114

Zuweisen von Notes Gruppen an Notes Benutzerkonten

Im One Identity Manager können Notes Gruppen direkt oder indirekt an Notes Benutzerkonten zugewiesen werden.

Bei der indirekten Zuweisung werden Personen und Notes 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 Rollen aufnehmen und die Person ein Notes Benutzerkonto besitzt, dann wird dieses Benutzerkonto in die Notes Gruppen aufgenommen.

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

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

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

Ausführliche Informationen finden Sie in den folgenden Handbüchern.

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

Detaillierte Informationen zum Thema

- Voraussetzungen für indirekte Zuweisungen von Notes Gruppen an Notes Benutzerkonten auf Seite 100
- Notes Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 102
- Notes Gruppen an Geschäftsrollen zuweisen auf Seite 103
- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 107
- Notes Gruppen in Systemrollen aufnehmen auf Seite 104
- Notes Gruppen in den IT Shop aufnehmen auf Seite 105
- Notes Gruppen direkt an ein Notes Benutzerkonto zuweisen auf Seite 108

Voraussetzungen für indirekte Zuweisungen von Notes Gruppen an Notes Benutzerkonten

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

1. Für Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen ist die Zuweisung von Personen und Notes Gruppen erlaubt.

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

   Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

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

      - ODER -

      Wählen Sie im Manager in der Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.
   2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
      - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
      - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
   3. Speichern Sie die Änderungen.
2. Einstellungen für die Zuweisung von Notes Gruppen an Notes Benutzerkonten.
   - Die Notes Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.
   - Die Notes Benutzerkonten sind über die Spalte `UID_Person` (**Person**) mit einer Person verbunden.
   - Notes Benutzerkonten und Gruppen gehören zur selben Notes Domäne.

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

Verwandte Themen

- Notes Benutzerkonten erstellen und bearbeiten auf Seite 139
- Allgemeine Stammdaten für Notes Benutzerkonten auf Seite 141

Notes Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Gruppe an Abteilungen, Kostenstellen oder Standorte zu, damit die Gruppe 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 **HCL Domino > 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 nicht-rollenbasierter Anmeldung oder 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

- Voraussetzungen für indirekte Zuweisungen von Notes Gruppen an Notes Benutzerkonten auf Seite 100
- Notes Gruppen an Geschäftsrollen zuweisen auf Seite 103
- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 107
- Notes Gruppen in Systemrollen aufnehmen auf Seite 104
- Notes Gruppen in den IT Shop aufnehmen auf Seite 105
- One Identity Manager Benutzer für die Verwaltung einer Domino-Umgebung auf Seite 13

Notes Gruppen an Geschäftsrollen zuweisen

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

Weisen Sie eine Gruppe an Geschäftsrollen zu, damit die Gruppe 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 **HCL Domino > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Geschäftsrolle und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Um Gruppen an eine Geschäftsrolle zuzuweisen (bei nicht-rollenbasierter Anmeldung oder 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.
    - (Optional) 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

- Voraussetzungen für indirekte Zuweisungen von Notes Gruppen an Notes Benutzerkonten auf Seite 100
- Notes Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 102
- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 107
- Notes Gruppen in Systemrollen aufnehmen auf Seite 104
- Notes Gruppen in den IT Shop aufnehmen auf Seite 105
- One Identity Manager Benutzer für die Verwaltung einer Domino-Umgebung auf Seite 13

Notes Gruppen in Systemrollen aufnehmen

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

Mit dieser Aufgabe nehmen Sie eine Gruppe in Systemrollen auf.

Wenn Sie eine Systemrolle an Personen zuweisen, wird die Gruppe an alle Notes 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 **HCL Domino > 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

- Voraussetzungen für indirekte Zuweisungen von Notes Gruppen an Notes Benutzerkonten auf Seite 100
- Notes Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 102
- Notes Gruppen an Geschäftsrollen zuweisen auf Seite 103
- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 107
- Notes Gruppen in den IT Shop aufnehmen auf Seite 105

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 **HCL Domino > 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. Wählen Sie den Tabreiter **IT Shop Strukturen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppe an die IT Shop Regale zu.
6. Speichern Sie die Änderungen.

Um eine Gruppe aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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. Wählen Sie den Tabreiter **IT Shop Strukturen**.
5. Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppe aus den IT Shop Regalen.
6. Speichern Sie die Änderungen.

Um eine Gruppe aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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

- Voraussetzungen für indirekte Zuweisungen von Notes Gruppen an Notes Benutzerkonten auf Seite 100
- Allgemeine Stammdaten von Notes Gruppen auf Seite 166
- Notes Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 102
- Notes Gruppen an Geschäftsrollen zuweisen auf Seite 103
- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 107
- Notes Gruppen in Systemrollen aufnehmen auf Seite 104

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 Benutzerkonten direkt an eine Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.
   - (Optional) Um die angezeigten Benutzerkonten zu filtern, wählen Sie im Eingabefeld **Notes Domänen** eine Domäne aus.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Notes Gruppen direkt an ein Notes Benutzerkonto zuweisen auf Seite 108
- Notes Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 102
- Notes Gruppen an Geschäftsrollen zuweisen auf Seite 103

- Notes Gruppen in Systemrollen aufnehmen auf Seite 104
- Notes Gruppen in den IT Shop aufnehmen auf Seite 105
- Eigentümer an Notes Gruppen zuweisen auf Seite 175
- Administratoren an Notes Gruppen zuweisen auf Seite 176

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 die Gruppen direkt an Benutzerkonten zuweisen. Gruppen, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Um Gruppen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.
    - (Optional) 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

- Ausschlusslisten und Einschlusslisten für Notes Benutzerkonten pflegen auf Seite 158
- Mitgliedschaften in dynamischen Gruppen auf Seite 179
- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 107
- Notes Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 102

- Notes Gruppen an Geschäftsrollen zuweisen auf Seite 103
- Notes Gruppen in Systemrollen aufnehmen auf Seite 104
- Notes Gruppen in den IT Shop aufnehmen auf Seite 105

Wirksamkeit von Mitgliedschaften in Notes Gruppen

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: 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 18: Festlegen der ausgeschlossenen Gruppen (Tabelle `NDOGroupExclusion`)

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

Tabelle 19: 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 20: Ausgeschlossene Gruppen und wirksame Zuweisungen

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

Voraussetzungen

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

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

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

Um Gruppen auszuschließen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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 63**.

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

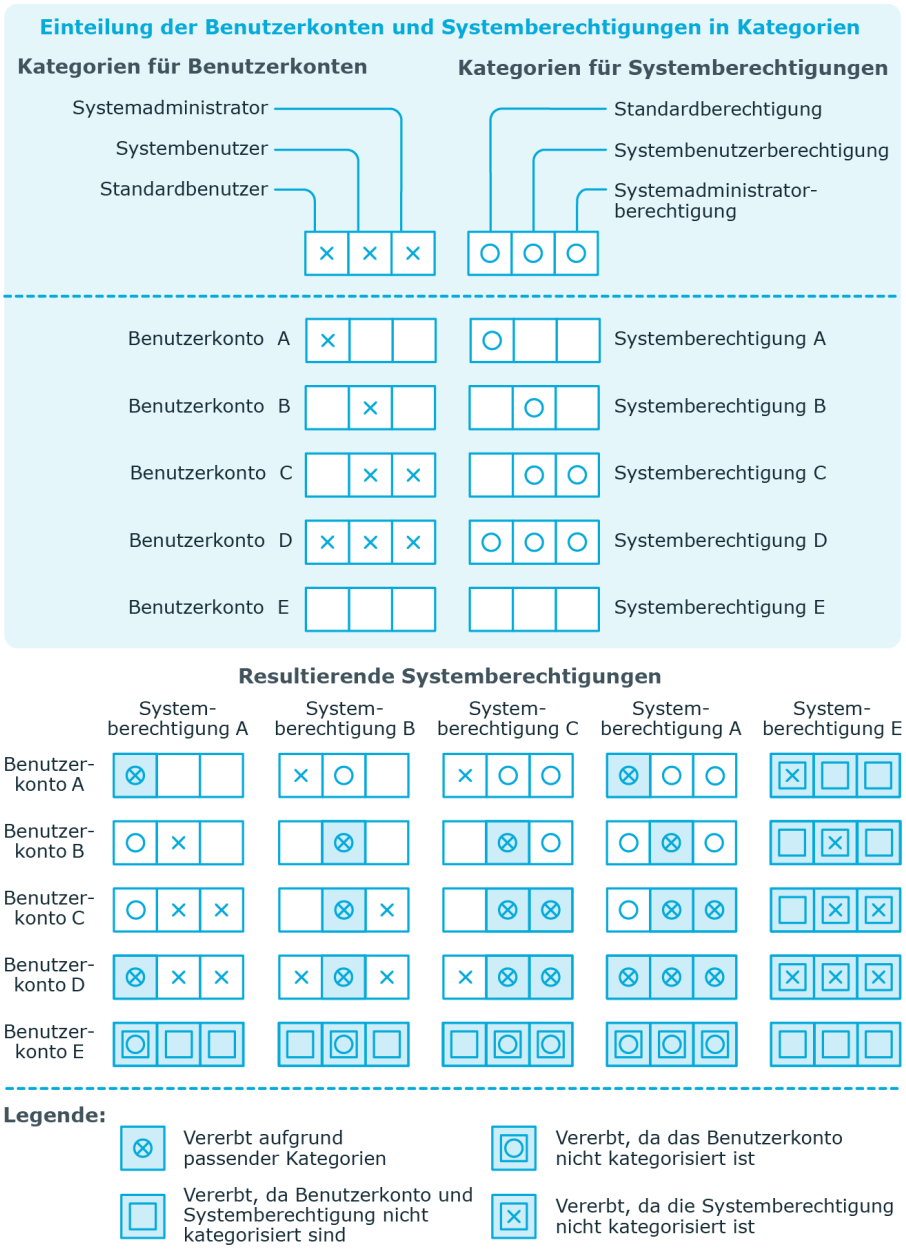
Benutzerkonto nicht in Kategorien eingestuft, dann wird die Gruppe ebenfalls an das Benutzerkonto vererbt.

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 21: 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

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

Verwandte Themen

- Kategorien für die Vererbung von Notes Gruppen definieren auf Seite 137
- Allgemeine Stammdaten für Notes Benutzerkonten auf Seite 141
- Allgemeine Stammdaten von Notes Gruppen auf Seite 166

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 22: 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.

5

Bereitstellen von Anmeldeinformationen für Notes Benutzerkonten

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

Detaillierte Informationen zum Thema

- Kennwortrichtlinien für Notes Benutzerkonten auf Seite 116
- Initiales Kennwort für neue Notes Benutzerkonten auf Seite 128
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 129

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 117
- Kennwortrichtlinien anwenden auf Seite 118
- Kennwortrichtlinien erstellen auf Seite 120
- Kennwortrichtlinien bearbeiten
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 124
- Ausschlussliste für Kennwörter auf Seite 127
- Kennwörter prüfen auf Seite 128
- Generieren eines Kennwortes testen auf Seite 128

Vordefinierte Kennwortrichtlinien

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

Kennwortrichtlinie für die Anmeldung am One Identity Manager

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

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

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

Kennwortrichtlinie für die Bildung des zentralen Kennwortes von Personen

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

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

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

Kennwortrichtlinien für Benutzerkonten

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

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

HINWEIS: Bei der Aktualisierung von One Identity Manager Version 7.x auf One Identity Manager Version 9.1 werden die Einstellung der Konfigurationsparameter zur Bildung von Kennwörtern auf die zielsystemspezifischen Kennwortrichtlinien umgesetzt.

Für Notes ist die Kennwortrichtlinie **HCL Domino 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.

Kennwortrichtlinien anwenden

Für Notes ist die Kennwortrichtlinie **HCL Domino 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 **HCL Domino > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Klicken Sie im Bereich **Zuweisungen** die Schaltfläche **Hinzufügen** und erfassen Sie folgende Daten.
    - **Anwenden auf**: Anwendungsbereich der Kennwortrichtlinie.

      Um den Anwendungsbereich festzulegen

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

Um die Zuweisung einer Kennwortrichtlinie zu ändern

1. Wählen Sie im Manager die Kategorie **HCL Domino > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.

4. Wählen Sie im Bereich **Zuweisungen** die Zuweisung, die Sie ändern möchten.
5. Wählen Sie in der Auswahlliste **Kennwortrichtlinie** die neu anzuwendende Kennwortrichtlinie.
6. Speichern Sie die Änderungen.

Kennwortrichtlinien erstellen

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

Um eine Kennwortrichtlinie zu erstellen

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kennwortrichtlinien auf Seite 121
- Richtlinieneinstellungen auf Seite 121
- Zeichenklassen für Kennwörter auf Seite 123
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 124
- Kennwortrichtlinien bearbeiten auf Seite 120

Kennwortrichtlinien bearbeiten

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

Um eine Kennwortrichtlinie zu bearbeiten

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kennwortrichtlinien auf Seite 121
- Richtlinieneinstellungen auf Seite 121
- Zeichenklassen für Kennwörter auf Seite 123
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 124
- Kennwortrichtlinien erstellen auf Seite 120

Allgemeine Stammdaten für Kennwortrichtlinien

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 23: Stammdaten einer Kennwortrichtlinie

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

Richtlinieneinstellungen

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

Tabelle 24: Richtlinieneinstellungen

Eigenschaft	Bedeutung
Initiales Kennwort	Initiales Kennwort für neu erzeugte Benutzerkonten. Wenn beim Erstellen eines Benutzerkontos kein Kennwort angegeben wird oder kein Zufallskennwort generiert wird, dann wird das initiale Kennwort benutzt.
Kennwortbestätigung	Kennwortwiederholung.
Min. Länge	Minimale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben muss. Ist der Wert **0**, ist kein Kennwort erforderlich.
Max. Länge	Maximale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben kann. Der maximal zulässige Wert ist **256**.
Max. Fehlanmeldungen	Anzahl der maximalen Fehlanmeldungen. Legen Sie die Anzahl der ungültigen Kennworteingaben fest. Die Anzahl der Fehlanmeldungen wird nur bei der Anmeldung am One Identity Manager berücksichtigt. Ist der Wert **0**, dann wird die Anzahl der Fehlanmeldungen nicht berücksichtigt. Die Angabe wird nur berücksichtigt, wenn die Anmeldung am One Identity Manager mit einem Systembenutzer- oder Personen-basierten Authentifizierungsmodul erfolgt. Hat ein Benutzer die Anzahl der maximalen Fehlanmeldungen überschritten, kann sich die Person oder der Systembenutzer nicht mehr am One Identity Manager anmelden. Kennwörter gesperrter Personen und Systembenutzer können im Kennwortrücksetzungsportal zurückgesetzt werden. Ausführliche Informationen finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.
Max. Tage gültig	Maximales Alter des Kennwortes. Geben Sie die Zeitspanne an, in der ein Kennwort verwendet werden kann, bevor ein neues Kennwort erwartet wird. Ist der Wert **0**, dann läuft das Kennwort nicht ab.
Kennwortchronik	Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert **5** eingegeben, werden die letzten fünf Kennwörter des Benutzers gespeichert. Ist der Wert **0**, dann werden keine Kennwörter in der Kennwortchronik gespeichert.
Min. Kennwortstärke	Gibt an, wie sicher ein Kennwort sein muss. Je höher die Kennwortstärke, desto sicherer ist das Kennwort. Mit dem Wert **0** wird die Kennwortstärke nicht geprüft. Die Werte **1**, **2**, **3** und **4** geben die erforderliche Komplexität des Kennwortes

Eigenschaft	Bedeutung
	an. Dabei stellt der Wert **1** die geringsten Anforderungen an die Komplexität eines Kennwortes. Der Wert **4** fordert die höchste Komplexität.
Namensbestandteile unzulässig	Gibt an, ob Namensbestandteile im Kennwort zulässig oder unzulässig sind. Ist die Option aktiviert, sind Namensbestandteile in Kennwörtern nicht zulässig. Es werden die Werte der Spalten berücksichtigt, für welche die Option **Enthält Namensbestandteile für die 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 25: Zeichenklassen für Kennwörter

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

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

Kundenspezifische Skripte für Kennwortanforderungen

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

Detaillierte Informationen zum Thema

- Skript zum Prüfen eines Kennwortes auf Seite 125
- Skript zum Generieren eines Kennwortes auf Seite 126

Skript zum Prüfen eines Kennwortes

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

Syntax für Prüfskripte

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

Mit Parametern:

`policy` = Kennwortrichtlinienobjekt

`spwd` = Kennwort, das zu prüfen ist

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

Beispiel: Skript zum Prüfen eines Kennwortes

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

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

Um ein kundenspezifisches Skript zum Prüfen eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **HCL Domino > 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 126

Skript zum Generieren eines Kennwortes

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

Syntax für Generierungsskripte

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

Mit Parametern:

`policy` = Kennwortrichtlinienobjekt

`spwd` = Generiertes Kennwort

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

Beispiel: Skript zum Generieren eines Kennwortes

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

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

```
      ' replace invalid characters at first position
      If pwd.Length>0
           If pwd(0)="?" Or pwd(0)="!"
                spwd.SetAt(0, CChar("_"))
           End If
      End If
End Sub
```

Um ein kundenspezifisches Skript zum Generieren eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **HCL Domino > 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 125

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.

Kennwörter prüfen

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

Um zu prüfen, ob ein Kennwort der Kennwortrichtlinie entspricht

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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 **HCL Domino > 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

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

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

Verwandte Themen

- Kennwortrichtlinien für Notes Benutzerkonten auf Seite 116
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 129

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.

6

Nutzung von AdminP-Aufträgen zur Verarbeitung von Domino-Prozessen

Domino 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 Änderungen im One Identity Manager 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?

Verwandte Themen

- Stammdaten von AdminP-Aufträgen auf Seite 132
- AdminP-Aufträge automatisch bestätigen auf Seite 132

AdminP-Aufträge automatisch bestätigen

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 **Domino: 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`

Verwandte Themen

- Nutzung von AdminP-Aufträgen zur Verarbeitung von Domino-Prozessen auf Seite 131

Stammdaten von AdminP-Aufträgen

Die Eigenschaften der synchronisierten AdminP-Aufträge werden im Manager angezeigt.

Um die Stammdaten eines Anforderungsdokuments anzuzeigen

- Wählen Sie im Manager die Kategorie **HCL Domino > Baumdarstellung > <Domäne> > AdminP-Aufträge > <Filter> > <Objekt> > <Aktion>**.

Tabelle 26: 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

Eigenschaft	Beschreibung
	soll.
Autor	Name des Autors des AdminP-Auftrags.
Datenbankdatei	Dateinamen der zu verarbeitenden Datenbanken.
Genehmigungskennzeichen	Gibt an, ob der AdminP-Auftrag durch einen Administrator genehmigt wurde.
Änderungskennzeichen	Gibt an, ob der AdminP-Auftrag geändert wurde.

Um die Stammdaten eines Antwortdokuments anzuzeigen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Baumdarstellung > <Domäne> > AdminP-Aufträge > <Filter> > <Objekt> > <Aktion>**.
2. Wählen Sie in der Ergebnisliste das Antwortdokument.

Tabelle 27: 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	Gibt an, ob bei der Verarbeitung des AdminP-Auftrags Fehler aufgetreten sind.

Verwandte Themen

- Nutzung von AdminP-Aufträgen zur Verarbeitung von Domino-Prozessen auf Seite 131
- AdminP-Aufträge automatisch bestätigen auf Seite 132

Abbilden von Notes Objekten im One Identity Manager

Mit dem One Identity Manager verwalten Sie alle Objekte der Domino-Umgebung, die für die Optimierung der Zugriffssteuerung im Zielsystem benötigt werden. Diese Objekte werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können im Manager angezeigt oder bearbeitet werden.

Detaillierte Informationen zum Thema

- Stammdaten von Notes Domänen bearbeiten auf Seite 135
- Notes Benutzerkonten auf Seite 138
- Notes Gruppen auf Seite 165
- Notes Zertifikate auf Seite 184
- Notes Schablonen auf Seite 189
- Notes Richtlinien auf Seite 190
- Notes Mail-In-Datenbanken auf Seite 195
- Notes Server auf Seite 201

Notes Domänen

Im One Identity Manager entspricht eine Domäne der Abbildung eines Sichtbarkeitsbereiches im Domino, beispielsweise einer produktiven Domino-Umgebung. Durch dieses Konstrukt, das im One Identity Manager wesentlich stringenter behandelt wird als im Domino, ist es möglich, mehrere produktive Domino-Umgebungen parallel mit einer One Identity Manager-Datenbank zu verwalten. Auch wenn im Domino 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.

Verwandte Themen

- Stammdaten von Notes Domänen bearbeiten auf Seite 135
- Kategorien für die Vererbung von Notes Gruppen definieren auf Seite 137
- Synchronisationsprojekt für eine Notes Domäne bearbeiten auf Seite 138
- Suchkriterien für die automatische Personenzuordnung bearbeiten auf Seite 86
- Einzelobjekte synchronisieren auf Seite 53

Stammdaten von Notes Domänen bearbeiten

Um die Stammdaten einer Notes Domäne zu bearbeiten

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

Verwandte Themen

- Allgemeine Stammdaten für Notes Domänen auf Seite 135
- Kategorien für die Vererbung von Notes Gruppen definieren auf Seite 137

Allgemeine Stammdaten für Notes Domänen

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

Tabelle 28: Allgemeine Stammdaten einer Notes Domäne

Eigenschaft	Beschreibung
Vollständiger Name	Vollständiger Name der Domäne.
Anzeigename	Anzeigename zur Anzeige der Domäne in der Benutzeroberfläche.
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

Eigenschaft	Beschreibung
	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 29: Zulässige Werte** **Wert** / **Synchronisation durch** / **Provisionierung durch** One Identity Manager / Domino Konnektor / Domino Konnektor Keine Synchronisation / keine / keine HINWEIS: Wenn Sie **Keine Synchronisation** festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.
Pfad der Benutzer-ID-Dateien	Pfad auf dem Gateway Server, der zur Erstellung neuer Benutzer-ID-Dateien genutzt wird. Weitere Informationen finden Sie unter Benutzer-ID-Dateien erzeugen und speichern auf Seite 48.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Eigenschaft	Beschreibung
ID-Vault aktiv	Gibt an, ob zum Wiederherstellen der Benutzer-ID-Dateien die ID-Vault-Funktion von Domino genutzt wird.

Verwandte Themen

- Kontendefinitionen für Notes Benutzerkonten auf Seite 62
- Notes Kontendefinitionen an Zielsysteme zuweisen auf Seite 80
- Zielsystemverantwortliche für Domino-Umgebungen auf Seite 242
- Wiederherstellen der Benutzer-ID-Dateien auf Seite 159

Kategorien für die Vererbung von Notes Gruppen definieren

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 63**.

Um Kategorien zu definieren

1. Wählen Sie im Manager in der Kategorie **HCL Domino > 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 111

Synchronisationsprojekt für eine Notes Domäne 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 im Manager die Kategorie **HCL Domino > Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten**.

Verwandte Themen

- Anpassen der Synchronisationskonfiguration für Domino-Umgebungen auf Seite 35

Notes Benutzerkonten

Mit dem One Identity Manager verwalten Sie die Benutzer und Personendokumente einer Domino-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

- Notes Benutzerkonten erstellen und bearbeiten auf Seite 139
- Unterstützte Typen von Benutzerkonten auf Seite 90
- Managen von Notes Benutzerkonten und Personen auf Seite 61
- Notes Gruppen direkt an ein Notes Benutzerkonto zuweisen
- Zusatzeigenschaften an Notes Benutzerkonten zuweisen auf Seite 151
- Notes Benutzerkonten als Eigentümer für Dokumente festlegen auf Seite 152
- Eigentümer an Notes Benutzerkonten zuweisen auf Seite 154
- Notes Benutzerkonten als Administrator für Dokumente festlegen auf Seite 155
- Administratoren an Notes Benutzerkonten zuweisen auf Seite 157
- Ausschlusslisten und Einschlusslisten für Notes Benutzerkonten pflegen auf Seite 158
- Überblick über Notes Benutzerkonten anzeigen auf Seite 159
- Wiederherstellen der Benutzer-ID-Dateien auf Seite 159
- Notes Benutzerkonten sperren und entsperren auf Seite 162
- Notes Benutzerkonten löschen und wiederherstellen auf Seite 164
- Benutzertyp festlegen auf Seite 46
- Postfachdateien erzeugen auf Seite 47
- Benutzer-ID-Dateien erzeugen und speichern auf Seite 48

Notes Benutzerkonten erstellen und bearbeiten

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 **HCL Domino > 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 **HCL Domino > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Benutzerkontos.
5. Speichern Sie die Änderungen.

Um ein Benutzerkonto für eine Person manuell zuzuweisen

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Notes Benutzerkonten auf Seite 141
- Zusätzliche Stammdaten von Notes Benutzerkonten auf Seite 147
- E-Mail-System von Notes Benutzerkonten auf Seite 145
- Adressangaben von Notes Benutzerkonten auf Seite 147
- Administrative Daten von Notes Benutzerkonten auf Seite 149

Verwandte Themen

- Kontendefinitionen für Notes Benutzerkonten auf Seite 62
- Unterstützte Typen von Benutzerkonten auf Seite 90
- Managen von Notes Benutzerkonten und Personen auf Seite 61
- Bereitstellen von Anmeldeinformationen für Notes Benutzerkonten auf Seite 116

Allgemeine Stammdaten für Notes Benutzerkonten

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

Tabelle 30: 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 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.
Keine Verbindung mit einer Person erforderlich	Gibt an, ob dem Benutzerkonto absichtlich keine Person zugeordnet ist. Die Option wird automatisch aktiviert, wenn ein Benutzerkonto in der Ausschlussliste für die automatische Personenzuordnung enthalten ist oder eine entsprechende Attestierung erfolgt ist. Sie können die Option manuell setzen. Aktivieren Sie die Option, falls das Benutzerkonto mit keiner Person verbunden werden muss (beispielsweise, wenn mehrere Personen das Benutzerkonto verwenden). Wenn durch die Attestierung diese Benutzerkonten genehmigt werden, werden diese Benutzerkonten künftig nicht mehr zur Attestierung vorgelegt. Im Web Portal können Benutzerkonten, die nicht mit einer Person verbunden sind, nach verschiedenen Kriterien gefiltert werden.
Nicht mit einer Person verbunden	Zeigt an, warum für das Benutzerkonto die Option **Keine Verbindung mit einer Person erforderlich** aktiviert ist. Mögliche Werte sind: • **durch Administrator**: Die Option wurde manuell durch den Administrator aktiviert.

Eigenschaft	Beschreibung
	• **durch Attestierung**: Das Benutzerkonto wurde attestiert. • **durch Ausschlusskriterium**: Das Benutzerkonto wird aufgrund eines Ausschlusskriteriums nicht mit einer Person verbunden. Das Benutzerkonto ist beispielsweise in der Ausschlussliste für die automatische Personenzuordnung enthalten (Konfigurationsparameter **PersonExcludeList**).
Kontendefinition	Kontendefinition, über die das Benutzerkonto erstellt wurde. Die Kontendefinition wird benutzt, um die Stammdaten des Benutzerkontos automatisch zu befüllen und um einen Automatisierungsgrad für das Benutzerkonto festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Person und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein. HINWEIS: Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden. HINWEIS: Über die Aufgabe **Entferne Kontendefinition** am Benutzerkonto können Sie das Benutzerkonto wieder in den Zustand **Linked** zurücksetzen. Dabei wird die Kontendefinition vom Benutzerkonto und von der Person entfernt. Das Benutzerkonto bleibt über diese Aufgabe erhalten, wird aber nicht mehr über die Kontendefinition verwaltet. Die Aufgabe entfernt nur Kontendefinitionen, die direkt zugewiesen sind (`XOrigin=1`). 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.

Eigenschaft	Beschreibung
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. 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 Domino-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

Eigenschaft	Beschreibung
	und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Benutzerkonto ist deaktiviert	Gibt an, 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 Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen. • **Persönliche Administratoridentität**: Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird. • **Zusatzidentität**: Benutzerkonto, das für einen spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken. • **Gruppenidentität**: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird. Weisen Sie alle Personen zu, die das Benutzerkonto nutzen. • **Dienstidentität**: Dienstkonto.
Privilegiertes Benutzerkonto	Gibt an, ob es sich um ein privilegiertes Benutzerkonto handelt.
Gruppen erbbar	Gibt an, ob das Benutzerkonto Gruppen über die verbundene Person erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Person Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Person eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Gruppe nur, wenn die Option aktiviert ist.

Verwandte Themen

- Kontendefinitionen für Notes Benutzerkonten auf Seite 62
- Managen von Notes Benutzerkonten und Personen auf Seite 61
- Unterstützte Typen von Benutzerkonten auf Seite 90
- E-Mail-System von Notes Benutzerkonten auf Seite 145
- Kategorien für die Vererbung von Notes Gruppen definieren auf Seite 137
- Notes Benutzerkonten sperren und entsperren auf Seite 162

E-Mail-System von Notes Benutzerkonten

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 31: 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

E-Mail-System	Eigenschaft	Beschreibung
		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 | DefTemplatePath** 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 POP or IMAP	Nachrichtenspeicherung	Sichtbarkeitsbereich des Postfachspeichers. Zur Auswahl stehen: • **0 - Notes** • **1 - Notes and Internet Mail** • **2 - Internet Mail**
Notes cc:Mail Other Other	Internetadresse	Vollständige SMTP-Adresse des Benutzerkontos. Die Internetadresse dient zur Identifizierung des Nachrichtenempfängers, wenn in der Domino-Umgebung Nachrichten über SMTP empfangen werden. Abhängig vom

E-Mail-System	Eigenschaft	Beschreibung
Internet Mail POP or IMAP		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

- Postfachdateien erzeugen auf Seite 47

Adressangaben von Notes Benutzerkonten

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 von Notes Benutzerkonten

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 **Domino: Größe der Postfachdateien einlesen**.

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

Tabelle 32: 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 Domino 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 116

Administrative Daten von Notes Benutzerkonten

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

Tabelle 33: 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 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.

Eigenschaft	Beschreibung
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 zufällig generiertes initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen. Das Kennwort wird nach dem Publizieren in das Zielsystem aus der Datenbank gelöscht. 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	Gibt an, 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 - HCL Domino** • **1 - HCL Domino Mail** • **2 - HCL Domino Desktop** • **3 - HCL Domino Designer** • **4 - HCL Domino Administration** • **5 - HCL iNotes®/Domino® CAL** Beim Anlegen eines neuen Benutzerkontos wird standardmäßig der Lizenztyp **0 - HCL Domino** übernommen.
Setup Profil	Name des Benutzerkonfigurationsprofils, das bei der Einrichtung der Arbeitsumgebung verwendet wird.
Abgleich mit fremdem	Gibt an, ob der Benutzername mit anderen Systemen

Eigenschaft	Beschreibung
Verzeichnis erlaubt	synchronisiert werden kann.
Netzwerk-Benutzerkonto	Benutzerkonto, welches zur Synchronisation zwischen Domino 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 **Domino: 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 201
- Kennwortrichtlinien für Notes Benutzerkonten auf Seite 116
- Initiales Kennwort für neue Notes Benutzerkonten auf Seite 128

Zusatzeigenschaften an Notes Benutzerkonten zuweisen

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

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

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

Notes Benutzerkonten als 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 ein Benutzerkonto als Eigentümer für Benutzerkonten festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um ein Benutzerkonto als Eigentümer für Gruppen festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um ein Benutzerkonto als Eigentümer für Mail-In-Datenbanken festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Mail-In-Datenbanken entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Mail-In-Datenbank und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um ein Benutzerkonto als Eigentümer für Zertifikate festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Zertifikat und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um ein Benutzerkonto als Eigentümer für Serverdokumente festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie das Serverdokument und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Eigentümer an Notes Benutzerkonten zuweisen

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

Um Benutzerkonten als Eigentümer festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Gruppen als Eigentümer festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Notes Benutzerkonten als Administrator für Dokumente festlegen

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

Um das Benutzerkonto als Administrator für Benutzerkonten festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um das Benutzerkonto als Administrator für Gruppen festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um das Benutzerkonto als Administrator für Mail-In-Datenbanken festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Mail-In-Datenbanken entfernen.

Um eine Zuweisung zu entfernen

- Wählen Sie die Mail-In-Datenbank und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um das Benutzerkonto als Administrator für Zertifikate festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Zertifikat und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um das Benutzerkonto als Administrator für Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Server und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um das Benutzerkonto als Administrator für Serverdokumente festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie das Serverdokument und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Administratoren an Notes Benutzerkonten zuweisen

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

Um Benutzerkonten als Administratoren festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Gruppen als Administratoren festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Ausschlusslisten und Einschlusslisten für Notes Benutzerkonten 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 im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um ein Benutzerkonto in die Ausschlussliste dynamischer Gruppen aufzunehmen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Mitgliedschaften in dynamischen Gruppen auf Seite 179

Überblick über Notes Benutzerkonten anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einem Benutzerkonto.

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie im Manager die Kategorie **HCL Domino > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das Notes Benutzerkonto**.

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. Domino stellt dafür seit der 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 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.

Detaillierte Informationen zum Thema

- Benutzer-ID-Dateien über ID-Vault wiederherstellen auf Seite 159
- Benutzer-ID-Dateien über ID-Restore wiederherstellen auf Seite 161

Benutzer-ID-Dateien über ID-Vault wiederherstellen

Die ID-Vault ist eine Domino Datenbank, die Kopien der Benutzer-ID-Dateien speichert. Damit ist Domino 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 227.
- 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 Domino-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 Domino-Umgebung.

Um ID-Vault zu nutzen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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 Domino 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 Domino-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 im Manager die Kategorie **HCL Domino > 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 Notes Client angemeldet, wird die lokale ID-Datei des Benutzers durch die aktualisierte Kopie aus der ID-Vault ersetzt. Beim nächsten Start des Notes Clients muss der Benutzer sich mit dem initialen Kennwort anmelden. Ist der Benutzer nicht am 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.

Benutzer-ID-Dateien über ID-Restore wiederherstellen

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 im Manager die Kategorie **HCL Domino > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **ID-Restore**.

   Der Prozess zur ID-Wiederherstellung führt folgende Schritte aus:

   - Löschen des aktuellen Personendokuments aus dem Domino-Verzeichnis.
   - Kopieren des initialen Personendokuments aus der Archivdatenbank in das Domino-Verzeichnis.
   - 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

- Archivdatenbank zur Sicherung der Personendokumente anlegen auf Seite 27

Notes Benutzerkonten sperren und entsperren

Ein Benutzerkonto gilt in einer Domino-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 **HCL Domino > 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 **HCL Domino > 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 im Manager die Kategorie **HCL Domino > 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 177

Verwandte Themen

- Kontendefinitionen für Notes Benutzerkonten auf Seite 62
- Automatisierungsgrade erstellen auf Seite 68

Notes Benutzerkonten löschen und wiederherstellen

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

Ein Benutzerkonto, das nicht über eine Kontendefinition entstanden ist, löschen Sie über die Ergebnisliste oder über die Menüleiste. Nach Bestätigung der Sicherheitsabfrage wird das Benutzerkonto im One Identity Manager zunächst zum Löschen markiert. 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.

Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Um ein Benutzerkonto zu löschen, das nicht über eine Kontendefinition verwaltet wird

1. Wählen Sie im Manager die Kategorie **HCL Domino > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Um ein Benutzerkonto wiederherzustellen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.

3. Klicken Sie in der Ergebnisliste .

Verwandte Themen

- Notes Benutzerkonten sperren und entsperren auf Seite 162
- Löschverzögerung für Notes Benutzerkonten festlegen auf Seite 97

Notes Gruppen

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

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

Detaillierte Informationen zum Thema

- Notes Gruppen erstellen auf Seite 166
- Stammdaten für Notes Gruppen bearbeiten auf Seite 166
- Notes Gruppen löschen auf Seite 183
- Sperrgruppen auf Seite 177
- Dynamische Gruppen auf Seite 178
- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 107
- Notes Mail-In-Datenbanken an Notes Gruppen zuweisen auf Seite 168
- Notes Server an Notes Gruppen zuweisen auf Seite 169
- Notes Gruppen in Notes Gruppen aufnehmen auf Seite 170
- Notes Gruppen als Eigentümer für Dokumente festlegen auf Seite 171
- Notes Gruppen als Administrator für Dokumente festlegen auf Seite 173
- Eigentümer an Notes Gruppen zuweisen auf Seite 175
- Administratoren an Notes Gruppen zuweisen auf Seite 176
- Zusatzeigenschaften an Notes Gruppen zuweisen auf Seite 176
- Überblick über Notes Gruppen anzeigen auf Seite 177

Notes Gruppen erstellen

Um eine Gruppe zu erstellen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Gruppen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten von Notes Gruppen auf Seite 166

Verwandte Themen

- Notes Gruppen löschen auf Seite 183
- Stammdaten für Notes Gruppen bearbeiten auf Seite 166

Stammdaten für Notes Gruppen bearbeiten

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie im Manager die Kategorie **HCL Domino > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten von Notes Gruppen auf Seite 166

Verwandte Themen

- Notes Gruppen löschen auf Seite 183
- Notes Gruppen erstellen auf Seite 166

Allgemeine Stammdaten von Notes Gruppen

Für Gruppen bearbeiten Sie folgende Stammdaten.

Tabelle 34: 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	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 im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen. Gruppen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Dynamische Mitglieder einlesen	Methode zum Festlegen der Mitglieder einer dynamischen Gruppe. • **Home server**: Die Gruppenmitglieder werden dynamisch aus den Mitgliedern des Homeservers ermittelt. Für diese Gruppe werden die Ausschluss- und die Einschlussliste synchronisiert. • **Keine**: Die Gruppe ist keine dynamische Gruppe.

Eigenschaft	Beschreibung
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Abgleich mit fremdem Verzeichnis erlaubt	Gibt an, ob Informationen über diese Gruppe an fremde Verzeichnisse weitergeschickt werden dürfen.
Sperrgruppe	Gibt an, ob die Gruppe als Sperrgruppe genutzt wird.
IT Shop	Gibt an, ob die Gruppe über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden. Die Option kann nicht aktiviert werden, wenn die Gruppe eine dynamische Gruppe ist.
Verwendung nur im IT Shop	Gibt an, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.
Dynamische Gruppe	Gibt an, 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 179
- Dynamische Gruppen auf Seite 178
- Sperrgruppen auf Seite 177
- Kategorien für die Vererbung von Notes Gruppen definieren auf Seite 137
- Notes Gruppen in den IT Shop aufnehmen auf Seite 105

Notes Mail-In-Datenbanken an Notes Gruppen zuweisen

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

Um Mail-In-Datenbanken an eine Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.
    - (Optional) Um die angezeigten Mail-In-Datenbanken zu filtern, wählen Sie im Eingabefeld **Notes Domänen** eine Domäne aus.

    TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Mail-In-Datenbanken entfernen.

    Um eine Zuweisung zu entfernen

    - Wählen Sie die Mail-In-Datenbank und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 107
- Notes Server an Notes Gruppen zuweisen auf Seite 169
- Notes Gruppen in Notes Gruppen aufnehmen auf Seite 170
- Mail-In-Datenbanken an Notes Gruppen zuweisen auf Seite 197

Notes Server an Notes Gruppen zuweisen

Notes Server können direkt an eine Gruppe zugewiesen werden.

Um Server an eine Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.
    - (Optional) Um die angezeigten Server zu filtern, wählen Sie im Eingabefeld **Notes Domänen** eine Domäne aus.

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

    Um eine Zuweisung zu entfernen

    - Wählen Sie den Server und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 107
- Notes Mail-In-Datenbanken an Notes Gruppen zuweisen auf Seite 168
- Notes Gruppen in Notes Gruppen aufnehmen auf Seite 170

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 im Manager die Kategorie **HCL Domino > 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.
    - (Optional) 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 untergeordnete Gruppe und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Um übergeordnete Gruppen an eine Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.
    - (Optional) 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 übergeordnete Gruppe und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Notes Benutzerkonten direkt an eine Notes Gruppe zuweisen auf Seite 107
- Notes Server an Notes Gruppen zuweisen auf Seite 169
- Notes Mail-In-Datenbanken an Notes Gruppen zuweisen auf Seite 168

Notes Gruppen als Eigentümer für Dokumente festlegen

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 im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um eine Gruppe als Eigentümer für Gruppen festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

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

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Mail-In-Datenbanken entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Mail-In-Datenbank und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Um eine Gruppe als Eigentümer für Zertifikate festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Zertifikat und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Um eine Gruppe als Eigentümer für Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Server und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Notes Gruppen als Administrator für Dokumente festlegen

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 im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um eine Gruppe als Administrator für Gruppen festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

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

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Mail-In-Datenbanken entfernen.

Um eine Zuweisung zu entfernen

- Wählen Sie die Mail-In-Datenbank und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um eine Gruppe als Administrator für Zertifikate festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Zertifikat und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um eine Gruppe als Administrator für Serverdokumente festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Serverdokument und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um eine Gruppe als Administrator für Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie den Server und doppelklicken Sie .

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 im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Gruppen als Eigentümer für eine Gruppe festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie .

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 im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen als Administratoren für eine Gruppe festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie .
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.

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

Um Zusatzeigenschaften für eine Gruppe festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

Überblick über Notes Gruppen anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Gruppe.

Um einen Überblick über eine Gruppe zu erhalten

1. Wählen Sie im Manager die Kategorie **HCL Domino > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die Notes Gruppe**.

Sperrgruppen

Ein Benutzerkonto gilt in einer Domino-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 Domino-Umgebung bereits Sperrgruppen vorhanden, werden diese wie normale Gruppen behandelt.

Um diese Gruppen für Sperrprozesse im One Identity Manager zu verwenden

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

Dynamische Gruppen

Seit der 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.

Detaillierte Informationen zum Thema

- Erweiterungsgruppen auf Seite 179
- Mitgliedschaften in dynamischen Gruppen auf Seite 179
- Homeserver zuweisen auf Seite 180
- Ausschlussliste bearbeiten auf Seite 180
- Einschlussliste bearbeiten auf Seite 182
- Ausschlusslisten und Einschlusslisten für Notes Mail-In-Datenbanken pflegen auf Seite 200
- Ausschlusslisten und Einschlusslisten für Notes Benutzerkonten pflegen auf Seite 158

Erweiterungsgruppen

Domino 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 Domino 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 Domino-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*.

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 im Manager die Kategorie **HCL Domino > 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.
   - (Optional) Um die angezeigten Server zu filtern, wählen Sie im Eingabefeld **Notes Domänen** eine Domäne aus.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Server und doppelklicken Sie .
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 im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen aus einer dynamischen Gruppe auszuschließen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Server aus einer dynamischen Gruppe auszuschließen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Server und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Um Mail-In-Datenbanken aus einer dynamischen Gruppe auszuschließen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Mail-In-Datenbanken entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Mail-In-Datenbank und doppelklicken Sie .
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 im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen zusätzlich in eine dynamische Gruppe aufzunehmen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Server zusätzlich in eine dynamische Gruppe aufzunehmen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Server und doppelklicken Sie .

6. Speichern Sie die Änderungen.

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

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Mail-In-Datenbanken entfernen.

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Mail-In-Datenbank und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Notes Gruppen löschen

Die Gruppe wird endgültig aus der One Identity Manager-Datenbank und dem Domino-Adressbuch gelöscht.

Um eine Gruppe zu löschen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Notes Zertifikate

Mit dem One Identity Manager verwalten Sie die Zertifikate einer Domino-Umgebung. Diese werden in der One Identity Manager-Datenbank als Notes Zertifikate abgebildet. Es werden alle Zertifikate abgebildet, die im Domino-Verzeichnis bekannt sind.

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.

Detaillierte Informationen zum Thema

- Stammdaten für Notes Zertifikate bearbeiten auf Seite 184
- Eigentümer an Notes Zertifikate zuweisen auf Seite 186
- Administratoren an Notes Zertifikate zuweisen auf Seite 187
- Überblick über Notes Zertifikate anzeigen auf Seite 188
- Neu eingelesene Notes Zertifikate nachbehandeln auf Seite 188
- Notes Zertifikatsanforderungen anzeigen auf Seite 189

Stammdaten für Notes Zertifikate bearbeiten

Um die Stammdaten eines Zertifikats zu bearbeiten

1. Wählen Sie im Manager die Kategorie **HCL Domino > Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat.

3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Notes Zertifikate auf Seite 185
- Kontaktdaten von Notes Zertifikaten auf Seite 186

Allgemeine Stammdaten für Notes Zertifikate

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

Tabelle 35: 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	Gibt an, 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.

Eigenschaft	Beschreibung
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 36: 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.

Eigentümer an Notes Zertifikate 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 im Manager die Kategorie **HCL Domino > 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Gruppen als Eigentümer für ein Zertifikat festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Administratoren an Notes Zertifikate zuweisen

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

Um Benutzerkonten als Administratoren für ein Zertifikat festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Gruppen als Administratoren für ein Zertifikat festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Überblick über Notes Zertifikate anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einem Zertifikat.

Um einen Überblick über ein Zertifikat zu erhalten

1. Wählen Sie im Manager die Kategorie **HCL Domino > Zertifikate**.
2. Wählen Sie in der Ergebnisliste das Zertifikat.
3. Wählen Sie die Aufgabe **Überblick über das Notes Zertifikat**.

Neu eingelesene Notes Zertifikate nachbehandeln

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.
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.

Verwandte Themen

- Notes Zertifikate übernehmen auf Seite 23
- Allgemeine Stammdaten für Notes Zertifikate auf Seite 185

Notes Zertifikatsanforderungen anzeigen

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 im Manager die Kategorie **HCL Domino > 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 37: 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.

Notes Schablonen

Mit dem One Identity Manager verwalten Sie die Schablonen einer Domino-Umgebung. Diese werden in der One Identity Manager-Datenbank als Notes Schablonen abgebildet. Es werden alle Schablonen abgebildet, die im Domino-Verzeichnis bekannt sind. Damit der Domino Konnektor im Zielsystem Benutzer anlegen kann, muss an den Benutzerkonten angegeben sein, welche Schablone beim Erzeugen der Postfachdatei für den Benutzer verwendet werden soll.

Um einen Überblick über eine Schablone zu erhalten

1. Wählen Sie im Manager die Kategorie **HCL Domino > Notes Schablonen**.
2. Wählen Sie in der Ergebnisliste die Schablone.
3. Wählen Sie die Aufgabe **Überblick über die Notes Schablone**.

Um die Stammdaten einer Schablone zu bearbeiten

1. Wählen Sie im Manager die Kategorie **HCL Domino > Notes Schablonen**.
2. Wählen Sie in der Ergebnisliste die Schablone.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
5. Speichern Sie die Änderungen.

Tabelle 38: Stammdaten einer Notes Schablone

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

Notes Richtlinien

Mit dem One Identity Manager verwalten Sie die Richtlinien einer Domino-Umgebung. Diese werden in der One Identity Manager-Datenbank als Notes Richtlinien abgebildet. Es werden alle Richtlinien abgebildet, die im Domino-Verzeichnis bekannt sind.

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

Detaillierte Informationen zum Thema

- Stammdaten von Notes Richtlinien anzeigen auf Seite 191
- Notes Richtlinieneinstellungen anzeigen auf Seite 192
- Mitglieder an Notes Richtlinien zuweisen auf Seite 192
- Eigentümer an Notes Richtlinien zuweisen auf Seite 193
- Administratoren an Notes Richtlinien zuweisen auf Seite 194
- Überblick über Notes Richtlinien anzeigen auf Seite 195

Stammdaten von Notes Richtlinien anzeigen

Um die Stammdaten von Richtlinien anzuzeigen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Richtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Detaillierte Informationen zum Thema

- Stammdaten für Notes Richtlinien auf Seite 191

Stammdaten für Notes Richtlinien

Folgende Informationen werden zu einer Richtlinie abgebildet.

Tabelle 39: 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	Gibt an, 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.

Notes Richtlinieneinstellungen anzeigen

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 im Manager die Kategorie **HCL Domino > Richtlinien**.
2. Wählen Sie in der Ergebnisliste eine Richtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie eine zugeordnete Richtlinieneinstellung und öffnen Sie das Kontextmenü dieser Zuordnung.
5. Klicken Sie **Gehe zum zugewiesenen Objekt**.
6. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Tabelle 40: 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

- Stammdaten für Notes Richtlinien auf Seite 191

Mitglieder an Notes Richtlinien zuweisen

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

Um Benutzerkonten an eine Richtlinie zuzuweisen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Richtlinie.
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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Gruppen an eine Richtlinie zuzuweisen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Richtlinie.
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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Eigentümer an Notes Richtlinien 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 im Manager die Kategorie **HCL Domino > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Richtlinie.
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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Gruppen als Eigentümer zuzuweisen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Richtlinie.
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.

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

   Um eine Zuweisung zu entfernen

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

Administratoren an Notes Richtlinien 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 im Manager die Kategorie **HCL Domino > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Richtlinie.
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.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen als Administratoren zuzuweisen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Richtlinie.
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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie ✓.

6. Speichern Sie die Änderungen.

Überblick über Notes Richtlinien anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Richtlinie.

Um einen Überblick über eine Richtlinie zu erhalten

1. Wählen Sie im Manager die Kategorie **HCL Domino > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Richtlinie.
3. Wählen Sie die Aufgabe **Überblick über die Notes Richtlinie**.

Notes Mail-In-Datenbanken

Mit dem One Identity Manager verwalten Sie die Mail-In-Datenbanken einer Domino-Umgebung. Diese werden in der One Identity Manager-Datenbank als Notes Mail-In-Datenbanken abgebildet. Es werden alle Mail-In-Datenbanken abgebildet, die im Domino-Verzeichnis bekannt sind.

Mail-In-Datenbanken können direkt an Gruppen zugewiesen werden und Mitglied dynamischer Gruppen sein. Den Mail-In-Datenbanken können Benutzerkonten und Gruppen als Eigentümer oder Administratoren zugewiesen werden.

Detaillierte Informationen zum Thema

- Notes Mail-In-Datenbanken erstellen auf Seite 196
- Stammdaten für Notes Mail-In-Datenbanken bearbeiten auf Seite 196
- Notes Mail-In-Datenbanken löschen auf Seite 201
- Überblick über Notes Mail-In-Datenbanken anzeigen auf Seite 201
- Mail-In-Datenbanken an Notes Gruppen zuweisen auf Seite 197
- Eigentümer an Notes Mail-In-Datenbanken zuweisen auf Seite 198
- Administratoren an Notes Mail-In-Datenbanken zuweisen auf Seite 199
- Ausschlusslisten und Einschlusslisten für Notes Mail-In-Datenbanken pflegen auf Seite 200

Notes Mail-In-Datenbanken erstellen

Um eine Mail-In-Datenbank zu erstellen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Mail-In-Datenbanken**.
2. Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Mail-In-Datenbank.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten von Notes Mail-In-Datenbanken auf Seite 197

Verwandte Themen

- Stammdaten für Notes Mail-In-Datenbanken bearbeiten auf Seite 196
- Notes Mail-In-Datenbanken löschen auf Seite 201

Stammdaten für Notes Mail-In-Datenbanken bearbeiten

Um die Stammdaten einer Mail-In-Datenbank zu bearbeiten

1. Wählen Sie im Manager die Kategorie **HCL Domino > Mail-In-Datenbanken**.
2. Wählen Sie in der Ergebnisliste die Mail-In-Datenbank.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten der Mail-In-Datenbank.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten von Notes Mail-In-Datenbanken auf Seite 197

Verwandte Themen

- Notes Mail-In-Datenbanken erstellen auf Seite 196
- Notes Mail-In-Datenbanken löschen auf Seite 201

Allgemeine Stammdaten von Notes Mail-In-Datenbanken

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

Tabelle 41: 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.
Nachrichtenspeicherung	Art der Nachrichtenspeicherung.
Abgleich mit fremdem Verzeichnis zulassen	Gibt an, ob Einträge der Mail-In-Datenbank in fremden Verzeichnissen eingesehen werden können.
Eingehende Post verschlüsseln	Gibt an, 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.

Mail-In-Datenbanken an Notes Gruppen 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 im Manager die Kategorie **HCL Domino > Mail-In-Datenbanken**.
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.

- (Optional) 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 Mail-In-Datenbanken an Notes Gruppen zuweisen auf Seite 168

Eigentümer an Notes Mail-In-Datenbanken 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 im Manager die Kategorie **HCL Domino > Mail-In-Datenbanken**.
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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Gruppen als Eigentümer festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Mail-In-Datenbanken**.
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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Administratoren an Notes Mail-In-Datenbanken 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 im Manager die Kategorie **HCL Domino > Mail-In-Datenbanken**.
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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Gruppen als Administratoren festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Mail-In-Datenbanken**.
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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Ausschlusslisten und Einschlusslisten für Notes Mail-In-Datenbanken 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 im Manager die Kategorie **HCL Domino > Mail-In-Datenbanken**.
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 Gruppen zu, in deren Einschlussliste die Mail-In-Datenbank aufgenommen werden soll.

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

   Um eine Zuweisung zu entfernen

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

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

1. Wählen Sie im Manager die Kategorie **HCL Domino > Mail-In-Datenbanken**.
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 Gruppen zu, in deren Ausschlussliste die Mail-In-Datenbank aufgenommen werden soll.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Mitgliedschaften in dynamischen Gruppen auf Seite 179

Überblick über Notes Mail-In-Datenbanken anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Mail-In-Datenbank.

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

1. Wählen Sie im Manager die Kategorie **HCL Domino > Mail-In-Datenbanken**.
2. Wählen Sie in der Ergebnisliste die Mail-In-Datenbank.
3. Wählen Sie die Aufgabe **Überblick über die Notes Mail-In-Datenbank**.

Notes Mail-In-Datenbanken löschen

Die Mail-In-Datenbank wird endgültig aus der One Identity Manager-Datenbank und dem Domino-Adressbuch gelöscht.

Um eine Mail-In-Datenbank zu löschen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Mail-In-Datenbanken**.
2. Wählen Sie in der Ergebnisliste die Mail-In-Datenbank.
3. Klicken Sie .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Notes Server

Mit dem One Identity Manager verwalten Sie die Server einer Domino-Umgebung. Diese werden in der One Identity Manager-Datenbank als Notes Server abgebildet. Es werden alle Server abgebildet, die im Domino-Verzeichnis bekannt sind.

Detaillierte Informationen zum Thema

- Stammdaten für Notes Server bearbeiten auf Seite 202
- Notes Server löschen auf Seite 230
- Notes Server an Notes Gruppen zuweisen auf Seite 205

- Mailserver an Notes Benutzerkonten zuweisen auf Seite 206
- Eigentümer an Serverdokumente zuweisen auf Seite 207
- Administratoren an Serverdokumente zuweisen auf Seite 208
- Administratoren mit voller Berechtigung an Notes Server zuweisen auf Seite 209
- Administratoren an Notes Server zuweisen auf Seite 210
- Datenbankadministratoren an Notes Server zuweisen auf Seite 211
- Administratoren mit voller Remotekonsolenberechtigung an Notes Server zuweisen auf Seite 212
- Leseberechtigte Administratoren an Notes Server zuweisen auf Seite 213
- Systemadministratoren an Notes Server zuweisen auf Seite 214
- Eingeschränkte Systemadministratoren an Notes Server zuweisen auf Seite 215
- Serverzugriff zulassen auf Seite 216
- Serverzugriff einschränken auf Seite 217
- Datenbanken und Schablonen erstellen auf Seite 218
- Neue Repliken erstellen auf Seite 220
- Routing über Server zulassen auf Seite 221
- Notes Server als Durchgangsziele für das Routing einrichten auf Seite 222
- Anruf durch Durchgangsserver veranlassen auf Seite 224
- Zulässige Ziele für Durchgangsserver auf Seite 225
- Unbeschränkte Methoden und Operationen signieren oder ausführen auf Seite 226
- Beschränkte LotusScript/Java-Agenten ausführen auf Seite 227
- Einfache Agenten und Formel-Agenten ausführen auf Seite 228
- Ausschlusslisten und Einschlusslisten pflegen auf Seite 229
- Überblick über Notes Server anzeigen auf Seite 230

Stammdaten für Notes Server bearbeiten

Um die Stammdaten eines Notes Servers zu bearbeiten

1. Wählen Sie im Manager die Kategorie **HCL Domino > Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten von Notes Servern auf Seite 203
- Standortdaten von Notes Servern auf Seite 204
- Sicherheitseinstellungen von Notes Servern auf Seite 205

Verwandte Themen

- Notes Server löschen auf Seite 230

Allgemeine Stammdaten von Notes Servern

Für Notes Server erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 42: 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 welcher 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. Weitere Informationen finden Sie unter Benutzer-ID-Dateien erzeugen und speichern auf Seite 48.
Hat Notes Postfachdateien	Gibt an, 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	Gibt an, 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	Gibt an, ob die Internetprotokollkonfiguration aus den Internet-Sites-Dokumenten im Domino-Verzeichnis geladen werden. Wenn die Option deaktiviert ist, werden diese Informationen

Eigenschaft	Beschreibung
	aus dem Serverdokument geladen.
SMTP-Service automatisch starten	Gibt an, 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	Gibt an, ob dieser Server als ID-Vault-Server genutzt wird.

Verwandte Themen

- Standortdaten von Notes Servern auf Seite 204
- Sicherheitseinstellungen von Notes Servern auf Seite 205
- Stammdaten für Notes Server bearbeiten auf Seite 202

Standortdaten von Notes Servern

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

Tabelle 43: Standortdaten eines Notes Servers

Eigenschaft	Beschreibung
Telefonnummer	Telefonnummer, 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	Gibt an, 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 44: Kontaktdaten eines Notes Servers

Eigenschaft	Beschreibung
Standort	Standort des Servers.

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

Verwandte Themen

- Allgemeine Stammdaten von Notes Servern auf Seite 203
- Sicherheitseinstellungen von Notes Servern auf Seite 205
- Stammdaten für Notes Server bearbeiten auf Seite 202

Sicherheitseinstellungen von Notes Servern

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

Tabelle 45: Sicherheitseinstellungen eines Notes Servers

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

Verwandte Themen

- Allgemeine Stammdaten von Notes Servern auf Seite 203
- Standortdaten von Notes Servern auf Seite 204
- Stammdaten für Notes Server bearbeiten auf Seite 202

Notes Server an Notes Gruppen zuweisen

Server können als Mitglieder in Gruppen aufgenommen werden.

Um einen Notes Server in Gruppen aufzunehmen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.
    - (Optional) 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 Server an Notes Gruppen zuweisen auf Seite 169

Mailserver an Notes 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 im Manager die Kategorie **HCL Domino > 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.

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

    Um eine Zuweisung zu entfernen

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

Verwandte Themen

- E-Mail-System von Notes Benutzerkonten auf Seite 145

Eigentümer an Serverdokumente 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 im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen als Eigentümer für ein Serverdokument festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Administratoren an Serverdokumente zuweisen

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

Um Benutzerkonten als Administratoren für ein Serverdokument festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen als Administratoren für ein Serverdokument festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Administratorzugriff festlegen

In der Domino-Umgebung können die Zugriffsrechte der Administratoren eingeschränkt werden. Administratoren erhalten dabei die Berechtigungen nur auf bestimmte Zugriffsebenen. Es können beispielsweise Datenbankadministratoren festgelegt oder einzelnen Administratoren volle Berechtigungen erteilt werden.

Administratoren mit voller Berechtigung an Notes Server zuweisen

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

Um Benutzerkonten als Vollzugriffadministratoren für einen Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen als Vollzugriffadministratoren für einen Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Administratorzugriff festlegen auf Seite 208
- Administratoren an Serverdokumente zuweisen auf Seite 208

Administratoren an Notes Server 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 für einen Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Um Gruppen als Administratoren für einen Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Datenbankadministratoren an Notes Server zuweisen auf Seite 211
- Administratoren mit voller Remotekonsolenberechtigung an Notes Server zuweisen auf Seite 212
- Administratorzugriff festlegen auf Seite 208
- Administratoren an Serverdokumente zuweisen auf Seite 208

Datenbankadministratoren an Notes Server zuweisen

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

Um Benutzerkonten als Datenbankadministratoren für einen Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen als Datenbankadministratoren für einen Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Administratorzugriff festlegen auf Seite 208
- Administratoren an Serverdokumente zuweisen auf Seite 208

Administratoren mit voller Remotekonsolenberechtigung an Notes Server zuweisen

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

Um Benutzerkonten als Remotekonsolenadministratoren für einen Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen als Remotekonsolenadministratoren für einen Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Leseberechtigte Administratoren an Notes Server zuweisen auf Seite 213
- Administratorzugriff festlegen auf Seite 208
- Administratoren an Serverdokumente zuweisen auf Seite 208

Leseberechtigte Administratoren an Notes Server zuweisen

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

Um Benutzerkonten als leseberechtigte Administratoren für einen Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen als leseberechtigte Administratoren für einen Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Administratorzugriff festlegen auf Seite 208
- Administratoren an Serverdokumente zuweisen auf Seite 208

Systemadministratoren an Notes Server zuweisen

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

Um Benutzerkonten als Systemadministratoren für einen Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen als Systemadministratoren für einen Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Eingeschränkte Systemadministratoren an Notes Server zuweisen auf Seite 215
- Administratorzugriff festlegen auf Seite 208
- Administratoren an Serverdokumente zuweisen auf Seite 208

Eingeschränkte Systemadministratoren an Notes Server zuweisen

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

Um Benutzerkonten als eingeschränkte Systemadministratoren für einen Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Um Gruppen als eingeschränkte Systemadministratoren für einen Server festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Systemadministratoren an Notes Server zuweisen auf Seite 214
- Administratorzugriff festlegen auf Seite 208
- Administratoren an Serverdokumente zuweisen auf Seite 208

Serverberechtigungen für Notes Server einrichten

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

Serverzugriff zulassen

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 Serverzugriff einschränken auf Seite 217.

Um Benutzerkonten den Serverzugriff explizit zu gewähren

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Um Gruppen den Serverzugriff explizit zu gewähren

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Servern den Serverzugriff explizit zu gewähren

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Server und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Verwandte Themen

- Serverberechtigungen für Notes Server einrichten auf Seite 216

Serverzugriff einschränken

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 zulassen auf Seite 216.

Um Benutzerkonten den Serverzugriff zu verweigern

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Gruppen den Serverzugriff zu verweigern

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Servern den Serverzugriff zu verweigern

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Server und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Verwandte Themen

- Serverberechtigungen für Notes Server einrichten auf Seite 216

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 im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Um Gruppen zu erlauben, Datenbanken und Schablonen zu erstellen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Servern zu erlauben, Datenbanken und Schablonen zu erstellen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Server und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Serverberechtigungen für Notes Server einrichten auf Seite 216

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 im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen zu erlauben, Repliken zu erstellen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Servern zu erlauben, Repliken zu erstellen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie den Server und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Verwandte Themen

- Serverberechtigungen für Notes Server einrichten auf Seite 216

Routing über Server zulassen

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 Notes Server als Durchgangsziele für das Routing einrichten auf Seite 222.

Um Benutzerkonten zu erlauben, den Server als Durchgangsserver zu nutzen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Gruppen zu erlauben, den Server als Durchgangsserver zu nutzen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Servern zu erlauben, den Server als Durchgangsserver zu nutzen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Server und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Verwandte Themen

- Serverberechtigungen für Notes Server einrichten auf Seite 216

Notes Server als Durchgangsziele für das Routing einrichten

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. Weitere Informationen finden Sie unter Serverzugriff zulassen auf Seite 216.

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 im Manager die Kategorie **HCL Domino > 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Gruppen zu erlauben, den Server als Durchgangsziel zu nutzen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Servern zu erlauben, den Server als Durchgangsziel zu nutzen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Server und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Verwandte Themen

- Serverberechtigungen für Notes Server einrichten auf Seite 216
- Routing über Server zulassen auf Seite 221

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 Notes Server als Durchgangsziele für das Routing einrichten auf Seite 222. Außerdem muss festgelegt sein, welche Benutzerkonten, Gruppen oder Server diesen Server als Durchgangsserver nutzen dürfen. Weitere Informationen finden Sie unter Routing über Server zulassen auf Seite 221.

Um Benutzerkonten zu erlauben, den Durchgangsserver für Wählverbindungen zu nutzen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen zu erlauben, den Durchgangsserver für Wählverbindungen zu nutzen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Servern zu erlauben, den Durchgangsserver für Wählverbindungen zu nutzen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Server und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Serverberechtigungen für Notes Server einrichten auf Seite 216

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 Notes Server als Durchgangsziele für das Routing einrichten auf Seite 222. Außerdem muss festgelegt sein, welche Benutzerkonten, Gruppen oder Server diesen Server als Durchgangsserver nutzen dürfen. Weitere Informationen finden Sie unter Routing über Server zulassen auf Seite 221.

Um die Zielserver für einen Durchgangsserver festzulegen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Server und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Serverberechtigungen für Notes Server einrichten auf Seite 216

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, auf einem Server unbeschränkte Methoden und Operationen auszuführen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen zu gestatten, auf einem Server unbeschränkte Methoden und Operationen auszuführen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Verwandte Themen

- Beschränkte LotusScript/Java-Agenten ausführen auf Seite 227
- Einfache Agenten und Formel-Agenten ausführen auf Seite 228
- Serverberechtigungen für Notes Server einrichten auf Seite 216

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, auf einem Server beschränkte LotusScript/Java-Agenten auszuführen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

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

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Verwandte Themen

- Unbeschränkte Methoden und Operationen signieren oder ausführen auf Seite 226
- Serverberechtigungen für Notes Server einrichten auf Seite 216

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, auf dem Server einfache und Formel-Agenten auszuführen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Benutzerkonto und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um Gruppen zu gestatten, auf dem Server einfache und Formel-Agenten auszuführen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Verwandte Themen

- Unbeschränkte Methoden und Operationen signieren oder ausführen auf Seite 226
- Serverberechtigungen für Notes Server einrichten auf Seite 216

Ausschlusslisten und Einschlusslisten pflegen

Notes Server können Mitglieder 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 im Manager die Kategorie **HCL Domino > 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 Gruppen zu, in deren Einschlussliste der Server aufgenommen werden soll.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Um einen Notes Server in die Ausschlussliste dynamischer Gruppen aufzunehmen

1. Wählen Sie im Manager die Kategorie **HCL Domino > 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 Gruppen zu, in deren Ausschlussliste der Server aufgenommen werden soll.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Mitgliedschaften in dynamischen Gruppen auf Seite 179

Überblick über Notes Server anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einem Notes Server.

Um einen Überblick über einen Notes Server zu erhalten

1. Wählen Sie im Manager die Kategorie **HCL Domino > Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Wählen Sie die Aufgabe **Überblick über den Notes Server**.

Notes Server löschen

Der Server wird endgültig aus der One Identity Manager-Datenbank und dem Domino-Adressbuch gelöscht.

Um einen Notes Servers zu löschen

1. Wählen Sie im Manager die Kategorie **HCL Domino > Notes Server**.
2. Wählen Sie in der Ergebnisliste den Server.
3. Klicken Sie .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Berichte über Notes Objekte

Der One Identity Manager stellt verschiedene Berichte zur Verfügung, in denen Informationen über das ausgewählte Basisobjekt und seine Beziehungen zu anderen

Objekten der One Identity Manager-Datenbank aufbereitet sind. Für Domino-Umgebungen stehen folgende Berichte zur Verfügung.

Tabelle 46: Berichte zur Datenqualität eines Zielsystems

Bericht	Bereitgestellt für	Beschreibung
Übersicht anzeigen	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Herkunft)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die Herkunft der zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Historie)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Gruppe	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, welche die ausgewählte Systemberechtigung besitzen.
Übersicht anzeigen	Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung und ihre Zuweisungen.
Übersicht anzeigen (inklusive Herkunft)	Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung und die Herkunft der zugewiesenen Benutzerkonten.
Übersicht anzeigen (inklusive Historie)	Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Zertifikat	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, deren Notes Benutzerkonto mit dem ausgewählten Zertifikat erstellt wurde.

Bericht	Bereitgestellt für	Beschreibung
Abweichende Systemberechtigungen anzeigen	Domäne	Der Bericht enthält alle Systemberechtigungen, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager.
Benutzerkonten anzeigen (inklusive Historie)	Domäne	Der Bericht liefert alle Benutzerkonten mit ihren Berechtigungen einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Benutzerkonten mit einer überdurchschnittliche Anzahl an Systemberechtigungen anzeigen	Domäne	Der Bericht enthält alle Benutzerkonten, die eine überdurchschnittliche Anzahl an Systemberechtigungen besitzen.
Personen mit mehreren Benutzerkonten anzeigen	Domäne	Der Bericht zeigt alle Personen, die mehrere Benutzerkonten besitzen. Der Bericht enthält eine Risikoeinschätzung.
Systemberechtigungen anzeigen (inklusive Historie)	Domäne	Der Bericht zeigt die Systemberechtigungen mit den zugewiesenen Benutzerkonten einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Domäne	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Zielsystem mindestens ein Benutzerkonto besitzen.
Ungenutzte Benutzerkonten anzeigen	Domäne	Der Bericht enthält alle Benutzerkonten, die in den letzten Monaten nicht verwendet wurden.
Unverbundene Benutzerkonten anzeigen	Domäne	Der Bericht zeigt alle Benutzerkonten, denen keine Person zugeordnet ist.

Tabelle 47: Zusätzliche Berichte für das Zielsystem

Bericht	Beschreibung
Notes Benutzerkonten- und Gruppenverteilung	Der Bericht enthält eine Zusammenfassung zur Benutzerkonten- und Gruppenverteilung aller Notes Domänen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager > Übersichten Zielsysteme**.
Datenqualität der Notes Benutzerkonten	Der Bericht enthält verschiedenen Auswertungen zur Datenqualität der Benutzerkonten aller Notes Domänen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager > Analyse Datenqualität**.

Verwandte Themen

- Übersicht aller Zuweisungen auf Seite 114

Behandeln von Notes Objekten im Web Portal

Der One Identity Manager bietet seinen Benutzern die Möglichkeit, verschiedene Aufgaben unkompliziert über ein Web Portal zu erledigen.

- Managen von Benutzerkonten und Personen

  Mit der Zuweisung einer Kontendefinition an ein IT Shop Regal kann die Kontendefinition von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Person, beispielsweise einen Manager, wird das Benutzerkonto angelegt.

- Managen von Zuweisungen von Gruppen

  Mit der Zuweisung einer Gruppe an ein IT Shop Regal kann die Gruppe von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Person wird die Gruppe zugewiesen.

  Manager und Administratoren von Organisationen können im Web Portal Gruppen an die Abteilungen, Kostenstellen oder Standorte zuweisen, für die sie verantwortlich sind. Die Gruppen werden an alle Personen vererbt, die Mitglied dieser Abteilungen, Kostenstellen oder Standorte sind.

  Wenn das Geschäftsrollenmodul vorhanden ist, können Manager und Administratoren von Geschäftsrollen im Web Portal Gruppen an die Geschäftsrollen zuweisen, für die sie verantwortlich sind. Die Gruppen werden an alle Personen vererbt, die Mitglied dieser Geschäftsrollen sind.

  Wenn das Systemrollenmodul vorhanden ist, können Verantwortliche von Systemrollen im Web Portal Gruppen an die Systemrollen zuweisen. Die Gruppen werden an alle Personen vererbt, denen diese Systemrollen zugewiesen sind.

- Attestierung

  Wenn das Modul Attestierung vorhanden ist, kann die Richtigkeit der Eigenschaften von Zielsystemobjekten und von Gruppenmitgliedschaften regelmäßig oder auf Anfrage bescheinigt werden. Dafür werden im Manager Attestierungsrichtlinien konfiguriert. Die Attestierer nutzen das Web Portal, um Attestierungsvorgänge zu entscheiden.

- Governance Administration

  Wenn das Modul Complianceregeln vorhanden ist, können Regeln definiert werden, die unzulässige Gruppenmitgliedschaften identifizieren und deren Risiken bewerten. Die Regeln werden regelmäßig und bei Änderungen an den Objekten im One Identity Manager überprüft. Complianceregeln werden im Manager definiert. Verantwortliche Personen nutzen das Web Portal, um Regelverletzungen zu überprüfen, aufzulösen und Ausnahmegenehmigungen zu erteilen.

  Wenn das Modul Unternehmensrichtlinien vorhanden ist, können Unternehmensrichtlinien für die im One Identity Manager abgebildeten Zielsystemobjekte definiert und deren Risiken bewertet werden. Unternehmensrichtlinien werden im Manager definiert. Verantwortliche Personen nutzen das Web Portal, um Richtlinienverletzungen zu überprüfen und Ausnahmegenehmigungen zu erteilen.

- Risikobewertung

  Über den Risikoindex von Gruppen kann das Risiko von Gruppenmitgliedschaften für das Unternehmen bewertet werden. Dafür stellt der One Identity Manager Standard-Berechnungsvorschriften bereit. Im Web Portal können die Berechnungsvorschriften modifiziert werden.

- Berichte und Statistiken

  Das Web Portal stellt verschiedene Berichte und Statistiken über die Personen, Benutzerkonten, deren Berechtigungen und Risiken bereit.

Ausführliche Informationen zu den genannten Themen finden Sie unter Zuweisen von Notes Gruppen an Notes Benutzerkonten auf Seite 99 und in folgenden Handbüchern:

- One Identity Manager Web Designer Web Portal Anwenderhandbuch
- One Identity Manager Administrationshandbuch für Attestierungen
- One Identity Manager Administrationshandbuch für Complianceregeln
- One Identity Manager Administrationshandbuch für Unternehmensrichtlinien
- One Identity Manager Administrationshandbuch für Risikobewertungen

Basisdaten für die Verwaltung einer Domino-Umgebung

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

- Kontendefinitionen

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

  Weitere Informationen finden Sie unter Kontendefinitionen für Notes Benutzerkonten auf Seite 62.

- 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 116.

- Zielsystemtypen

  Zielsystemtypen werden für die Konfiguration des Zielsystemabgleichs benötigt. An den Zielsystemtypen werden die Tabellen gepflegt, die ausstehende Objekte enthalten können. Es werden Einstellungen für die Provisionierung von Mitgliedschaften und die Einzelobjektsynchronisation vorgenommen. Zusätzlich dient der Zielsystemtyp zur Abbildung der Objekte im Unified Namespace.

  Weitere Informationen finden Sie unter Ausstehende Objekte nachbearbeiten auf Seite 54.

- Zielsystemverantwortliche

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

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

  Weitere Informationen finden Sie unter Zielsystemverantwortliche für Domino-Umgebungen auf Seite 242.

- Server

  Für die Verarbeitung der Domino-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 Jobserver für Domino-spezifische Prozessverarbeitung auf Seite 237.

Jobserver für Domino-spezifische Prozessverarbeitung

Für die Verarbeitung der Domino-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 **HCL Domino > 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 **HCL Domino > Basisdaten zur Konfiguration > Server**.
2. Wählen Sie in der Ergebnisliste den Jobserver-Eintrag.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

4. Bearbeiten Sie die Stammdaten für den Jobserver.
5. Wählen Sie die Aufgabe **Serverfunktionen zuweisen** und legen Sie die Serverfunktionen fest.
6. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Jobserver auf Seite 238
- Festlegen der Serverfunktionen auf Seite 241

Verwandte Themen

- One Identity Manager Service auf dem Gateway Server installieren auf Seite 24

Allgemeine Stammdaten für Jobserver

HINWEIS: Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten > Installationen > Jobserver** zur Verfügung.

HINWEIS: Abhängig von den installierten Modulen können weitere Eigenschaften verfügbar sein.

Tabelle 48: Eigenschaften eines Jobservers

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS Syntax. Syntax: `<Name des Servers>.<Vollqualifizierter Domänenname>`
Server ist Cluster	Gibt an, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. HINWEIS: Die Eigenschaften **Server ist Cluster** und **Server gehört zu Cluster** schließen einander aus.
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.
IP-Adresse (IPv4)	Internet Protokoll Version 4 (IPv4)-Adresse des Servers.
Kopierverfahren (Quellserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Quelle einer Kopieraktion ist. Derzeit werden nur Kopierverfahren über die Programme `Robocopy` und `rsync` unterstützt. Wird kein Verfahren angegeben, ermittelt der One Identity

Eigenschaft	Bedeutung
	Manager Service zur Laufzeit das Betriebssystem des Servers, auf dem die Kopieraktion ausgeführt wird. Die Replikation erfolgt dann zwischen Servern mit einem Windows Betriebssystem mit dem Programm `Robocopy` und zwischen Servern mit einem Linux Betriebssystem mit dem Programm `rsync`. Unterscheiden sich die Betriebssysteme des Quellservers und des Zielservers, so ist für eine erfolgreiche Replikation die Angabe der zulässigen Kopierverfahren zwingend erforderlich. Es wird das Kopierverfahren eingesetzt, das beide Server unterstützen.
Kopierverfahren (Zielserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Ziel einer Kopieraktion ist.
Codierung	Codierung des Zeichensatzes mit der Dateien auf dem Server geschrieben werden.
Übergeordneter Jobserver	Bezeichnung des übergeordneten Jobservers.
Ausführender Server	Bezeichnung des ausführenden Servers. Eingetragen wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden. Diese Angabe wird bei der automatischen Aktualisierung des One Identity Manager Service ausgewertet. Verarbeitet ein Server mehrere Queues, wird mit der Auslieferung von Prozessschritten solange gewartet, bis alle Queues, die auf demselben Server abgearbeitet werden, die automatische Aktualisierung abgeschlossen haben.
Queue	Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Mit dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Serverbetriebssystem	Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte **Win32**, **Windows**, **Linux** und **Unix**. Ist die Angabe leer, wird **Win32** angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen.

Eigenschaft	Bedeutung
One Identity Manager Service installiert	Gibt an, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur `QBM_PJobQueueLoad` aktiviert, sobald die Queue das erste Mal angefragt wird. Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.
Stopp One Identity Manager Service	Gibt an, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten. Den Dienst können Sie mit entsprechenden administrativen Berechtigungen im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*.
Pausiert wegen Nicht-verfügbarkeit eines Zielsystems	Gibt an, ob die Verarbeitung von Aufträgen für diese Queue angehalten wurde, weil das Zielsystem, für den dieser Jobserver der Synchronisationsserver ist, vorübergehend nicht erreichbar ist. Sobald das Zielsystem wieder erreichbar ist, wird die Verarbeitung gestartet und alle anstehenden Aufträge werden ausgeführt. Ausführliche Informationen zum Offline-Modus finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.
Kein automatisches Softwareupdate	Gibt an, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.
Softwareupdate läuft	Gibt an, ob gerade eine Softwareaktualisierung ausgeführt wird.
Serverfunktion	Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

Verwandte Themen

- Festlegen der Serverfunktionen auf Seite 241

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 49: 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.
HCL Domino Gateway Server	Gateway Server für die Synchronisation des One Identity Manager mit der HCL Domino-Umgebung.
HCL Domino Konnektor	Server, auf dem der HCL Domino Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem HCL Domino 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. 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

Serverfunktion	Anmerkungen
	verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.
CSV Skriptserver	Der Server kann CSV-Dateien per Prozesskomponente `ScriptComponent` verarbeiten.
Generischer 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.
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

- Allgemeine Stammdaten für Jobserver auf Seite 238

Zielsystemverantwortliche für Domino-Umgebungen

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

Wenn Sie die Berechtigungen 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 Notes 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 50: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Domino** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

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 > Domino**.
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 **HCL Domino > 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 **HCL Domino > 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 | Domino** 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 Domino-Umgebung auf Seite 13
- Allgemeine Stammdaten für Notes Domänen auf Seite 135

Anhang A

Konfigurationsparameter für die Verwaltung einer Domino-Umgebung

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

Tabelle 51: Konfigurationsparameter für die Verwaltung einer Domino-Umgebung

Konfigurationsparameter	Bedeutung bei Aktivierung
TargetSystem | NDO	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung des Zielsystems Domino. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
TargetSystem | NDO | Accounts	Parameter zur Konfiguration der Angaben zu Notes Benutzerkonten.
TargetSystem | NDO | Accounts | InitialRandomPassword	Gibt an, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in der zugewiesenen Kennwortrichtlinie definiert sind.
TargetSystem | NDO | Accounts | InitialRandomPassword	Person, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Geschäftsrolle, Verantwortlicher der

Konfigurationsparameter	Bedeutung bei Aktivierung
| SendTo	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	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Anmeldeinformationen zum Benutzerkonto zu versorgen. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto** verwendet.
TargetSystem | NDO | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Informationen zum initialen Kennwort zu versorgen. Es wird die Mailvorlage **Person - Initiales Kennwort für neues Benutzerkonto** verwendet.
TargetSystem | NDO | Accounts | MailFileAccessRole	Zugriffsstufe, welche für den Besitzer einer Postfachdatei gesetzt wird, wenn die Postfachdatei erstellt wird. Mögliche Wert sind **Manager**, **Editor**, **Designer**. Wenn der Konfigurationsparameter deaktiviert ist, wird die Zugriffsstufe **Manager** gesetzt.
TargetSystem | NDO | Accounts | MailTemplateDefaultValues	Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto mit Standardwerten** verwendet.
TargetSystem | NDO | BuildShortnameFullSync	Legt fest, ob bei der Synchronisation Kurznamen für Personendokumente erzeugt werden sollen, die in Domino 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 | DefaultAddress	Standard-E-Mail-Adresse des Empfängers von 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 |	Angabe der maximalen Anzahl von Mitgliedern pro Sperr-

Konfigurationsparameter	Bedeutung bei Aktivierung
DenyAccessGroups | Memberlimit	gruppe. 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 | 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	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 | PersonAutoDefault	Modus für die automatische Personenzuordnung für Benutzerkonten, 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	Modus für die automatische Personenzuordnung für Benutzerkonten, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem | NDO | PersonExcludeList	Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird. Beispiel: `ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $`
TargetSystem | NDO | UpdateAddressbook	Ist der Konfigurationsparameters aktiviert, werden beim Erzeugen neuer Benutzer-ID-Dateien auch Einträge im Domino-Verzeichnis erzeugt.
TargetSystem | NDO | VerifyUpdates	Gibt an, 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 Domino

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

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

Die Projektvorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 52: Abbildung der Notes Schematypen auf Tabellen im One Identity Manager Schema

Schematyp in Domino	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
PolicyRegistration	NDOPolicySetting
PolicySecurity	NDOPolicySetting

Schematyp in Domino	Tabelle im One Identity Manager Schema
PolicySetup	NDOPolicySetting
Server	NDOServer
Template	NDOTemplate

Anhang C

Verarbeitungsmethoden von Domino Systemobjekten

Folgende Tabelle beschreibt die zulässigen Verarbeitungsmethoden für die Domino Schematypen und benennt notwendige Einschränkungen bei der Verarbeitung der Systemobjekte.

Tabelle 53: Zulässige Verarbeitungsmethoden für Domino Schematypen

Schematyp	Lesen	Einfügen	Löschen	Aktualisieren
Admin4-Datenbank (`AdminRequest`)	Ja	Nein	Nein	Nein
Zertifikatsanforderung (`CertificateRequest`)	Ja	Nein	Nein	Nein
Zertifikat (`Certifier`)	Ja	Nein	Ja	Ja
Domäne (`CurrentDomain`)	Ja	Nein	Nein	Nein
Mail-In-Datenbank (`Database`)	Ja	Ja	Ja	Ja
Gruppe (`Group`)	Ja	Ja	Ja	Ja
Benutzerkonto (`Person`)	Ja	Ja	Ja	Ja
Richtlinieneinstellung (`PolicyArchive`)	Ja	Nein	Nein	Nein
Richtlinieneinstellung (`PolicyDesktop`)	Ja	Nein	Nein	Nein
Richtlinieneinstellung (`PolicyMail`)	Ja	Nein	Nein	Nein
Richtlinie (`PolicyMaster`)	Ja	Nein	Nein	Ja
Richtlinieneinstellung (`PolicyRegistration`)	Ja	Nein	Nein	Nein
Richtlinieneinstellung	Ja	Nein	Nein	Nein

Schematyp	Lesen	Einfügen	Löschen	Aktualisieren
(PolicySecurity)				
Richtlinieneinstellung (PolicySetup)	Ja	Nein	Nein	Nein
Server (Server)	Ja	Nein	Ja	Ja
Schablone (Template)	Ja	Nein	Nein	Nein

Anhang D

Einstellungen des Domino Konnektors

Für die Systemverbindung mit dem Domino Konnektor werden die folgenden Einstellungen konfiguriert.

Tabelle 54: Einstellungen des Domino Konnektors

Einstellung	Bedeutung
Domino-Server	Name des Domino-Servers, mit dem der Gateway Server kommuniziert. Variable: `CP_NDOserver`
Domino-Verzeichnis	Name des Domino-Verzeichnisses. Standardwert: **Names.nsf** Variable: `CP_NDOdatabasename`
Kundenspezifische INI-Datei	Name und Pfad zur kundenspezifischen INI-Datei. Standardwert: **C:\Program Files (x86)\IBM\Notes\vinotes.ini** Variable: `CP_NDOinifile`
Kennwort der ID-Datei	Kennwort der ID-Datei des Synchronisationsbenutzers. Der Pfad zu dieser ID-Datei muss in der kunden-spezifischen INI-Datei angegeben sein. Variable: `CP_BASEpassword`
Objekte über AdminP-Prozesse löschen	Gibt an, ob Notes Objekte über AdminP-Prozesse gelöscht werden sollen. Standardwert: **True** Variable: `CP_NDOuseadminpdel`
Domäne	Definierter Name der Notes Domäne. Variable: `CP_ADRootdn`

Einstellung	Bedeutung
Zugriffsstufe	Zugriffsstufe, welche für den Besitzer einer Postfachdatei gesetzt wird, wenn die Postfachdatei erstellt wird. Mögliche Wert sind **Manager**, **Editor**, **Designer**. Standardwert: **0** (Manager) Variable: `MailFileAccessType`
UserCreateMailDb	Gibt an, ob die Postfachdatei nach der Registrierung eines Notes Benutzers erzeugt wird. Dabei wird die Schablone verwendet, die am Benutzerkonto oder im Konfigurationsparameter **TargetSystem | NDO | DefTemplatePath** angegeben ist. Standardwert: **0** Variable: `UserCreateMailDb` Der Wert **1** gibt an, dass die Postfachdatei bereits während der Registrierung des Notes Benutzers erzeugt werden. In diesem Fall wird die Schablone des Notes Servers verwendet, auf dem der Benutzer registriert wird.
UserIDFilesDefaultPath	Standardpfad für das Speichern der Benutzer-ID-Dateien auf dem Gateway Server. Standardwert: **C:\Program Files (x86)\IBM\Lotus\Notes\Data\IDS** Variable: `UserIDFilesDefaultPath`
UserIsNorthAmerican	Gibt an, ob neu erzeugte ID-Dateien kompatibel zur US-amerikanischen und kanadischen Domino Version sind. Wert **1**: Alle neu erzeugten Benutzer-ID-Dateien werden mit nordamerikanischer Verschlüsselungsstärke berechnet. Standardwert: **0** Variable: `UserIsNorthAmerican`
UserMinPwdLen	Gibt die minimalen Kennwortlänge an, die in allen neu zu berechnenden Benutzer-ID-Dateien zu setzen ist. Standardwert: **0** Variable: `UserMinPwdLen`
UserStoreIDInAddressbook	Gibt an, ob die erstellte ID-Datei als Attachment an das Personendokument angehängt oder auf dem Gateway Server gespeichert wird. Standardwert: **0** - Die ID-Datei wird als Attachment an das Personendokument angehängt.

Einstellung	Bedeutung
	Variable: `UserStoreIDInAddressbook`
UserType	Typ des Benutzers, der durch eine Registrierung entsteht. Mögliche Werte sind **176** (FULL CLIENT USER), **175** (DESKTOP CLIENT USER), **174** (LIMITED CLIENT USER). Standardwert: **176** Variable: `UserType`

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

A

Administrator
- für Dokumente 173
- Mail-In-Datenbank 199
- Notes Benutzerkonto 157
- Notes Gruppe 173, 176
- Richtlinien 194
- Zertifikat 187

AdminP-Auftrag 131
- automatisch bestätigen 132
- genehmigen 132

Anforderungsdokument 132
Anmeldeinformationen 129
Antwortdokument 132
Anwendungsrolle 13
- Zielsystemverantwortliche 242

Architektur 11
Archivdatenbank
- anlegen 27

Ausnahmerichtlinie 190
Ausschlussdefinition 109
Ausschlussliste 179
- bearbeiten 180, 200, 229

Ausstehendes Objekt 54
Automatisierungsgrad
- bearbeiten 67
- erstellen 68

B

Basisobjekt 38, 44
Benachrichtigung 129
Benutzer-ID-Datei
- Ablaufdatum 149
- speichern 48
- verlängern 149
- wiederherstellen 159

Benutzerkonto
- administratives Benutzerkonto 93
- Automatisierungsgrad 89
- Bildungsregeln ausführen 73
- Datenqualität 230
- einrichten 139
- Gruppen zuweisen 108
- Gruppenidentität 95
- Identität 90
- Kategorie 111
- Kennwort 128
  - Benachrichtigung 129
- Person zuordnen 83
- persönliche Administratoridentität 94
- privilegiertes Benutzerkonto 90, 93, 96
- rezertifizieren 22
- Standardbenutzerkonto 92
- Typ 90, 92, 96
- ungenutzt 230
- verbunden 89
- zugewiesene Gruppen 230

Bericht
- Übersicht aller Zuweisungen 114

Bildungsregel
- IT Betriebsdaten ändern 73

C

CA-Prozess 185
Complianceprüfung 179

D

Domäne
  ID-Vault nutzen 159
  Kategorie 111
  Personenzuordnung 86
  Zielsystemverantwortlicher 13
Domino-Server
  Einstellungen 20
Domino-Umgebung
  Zielsystemverantwortlicher 242
Domino-Verzeichnis
  Filter 20
  Volltext-Index 20
Domino Server Version 16
Dynamische Gruppe
  Notes 178

E

E-Mail-Benachrichtigung 129
Eigentümer
  für Dokumente 171
  Mail-In-Datenbank 198
  Notes Benutzerkonto 152, 154
  Notes Gruppe 171, 175
  Richtlinien 193
  Zertifikat 186
Einschlussliste 179
  bearbeiten 182, 200, 229
Einzelobjekt synchronisieren 53
Einzelobjektsynchronisation 44, 53
  beschleunigen 45
Erweiterungsgruppe 179

G

Gateway Server 20, 237
  Archivdatenbank anlegen 27
  installieren 21
  konfigurieren 21
  One Identity Manager Service installieren 24
  Serverfunktion 241
Gruppe
  Abteilung zuweisen 102
  Geschäftsrollen zuweisen 103
  in IT Shop aufnehmen 105
  Kostenstelle zuweisen 102
  Sperrgruppe 162
  Standort zuweisen 102
  Systemrolle zuweisen 104
  Vererbung über Systemrollen 104
Gruppenidentität 95

I

ID-Datei
  Ablaufdatum 149
  speichern 48
  verlängern 149
  wiederherstellen 159
ID-Restore 161
ID-Vault 159
ID-Vault-Server 159, 203
Identität 90
INI-Datei erstellen 23

IT Betriebsdaten 70
ändern 73
Standardwert 70
IT Shop Regal
Gruppen zuweisen 105
Kontendefinitionen zuweisen 78

J

Java-Agent 227
Jobserver
Eigenschaften 238
für Domino 237
Lastverteilung 45

K

Kennwort
initial 128-129
Kennwortrichtlinie 116
Anzeigename 121
Ausschlussliste 127
bearbeiten 120
erstellen 120
Fehlanmeldungen 121
Fehlermeldung 121
Generierungsskript 124, 126
initiales Kennwort 121
Kennwort generieren 128
Kennwort prüfen 128
Kennwortalter 121
Kennwortlänge 121
Kennwortstärke 121
Kennwortzyklus 121
Namensbestandteile 121
neu 120
Prüfskript 124-125
Standardrichtlinie 118, 121
Vordefinierte 117
Zeichenklassen 123
zuweisen 118
Konfigurationsparameter
Domino 15, 246
Kontendefinition
an Benutzerkonten zuweisen 89
an Kunden-Umgebung zuweisen 80
an Person zuweisen 74
an Systemrollen zuweisen 77
Automatisierungsgrad bearbeiten 67
Automatisierungsgrad erstellen 68
bearbeiten 64
erstellen 63
für Notes Benutzerkonten 62
in IT Shop aufnehmen 78
IT Betriebsdaten 72
löschen 81
Kunden-Umgebung
Kontendefinition (initial) 80

L

Lastverteilung 45
LotusScript-Agent 227

M

Mail-In-Datenbank 195
Administrator 199
Administrator festlegen 173
Ausschlussliste 200
bearbeiten 196
Domäne 197

dynamische Gruppe 200
Eigentümer 198
Eigentümer festlegen 171
Einschlussliste 200
erstellen 196
löschen 201
Notes Gruppe zuweisen 197
Schablone 197
Server 197
Mitgliedschaft
Änderung provisionieren 42

N

NLog 57
Notes Benutzerkonto 138
Administrator festlegen 173
Administratoren 157
administrierbare Dokumente 155
Adressangabe 147
anonymisieren 162
Ausschlussliste bearbeiten 158
Dokumentenbesitz 152
E-Mail-System 145
Eigentümer 154
Eigentümer festlegen 171
Einschlussliste bearbeiten 158
entsperren 162
ID-Datei
wiederherstellen 161
ID-Vault 159
Rechte 159
Identität 141
Kategorie zuordnen 141
Kennwort 149
Kennwort zurücksetzen 159
Kennwortrichtlinien 149
Konfigurationsprofil 149
Kurzname 141
Lizenztyp 149
löschen 164
Löschverzögerung 97, 164
Person deaktivieren 162
Postfachdatei 145
Größe beschränken 147
logische Größe 147
physische Größe 147
privilegiertes Benutzerkonto 141
provisionieren 188
rezertifizieren 188
Risikoindex 141
Same Time Server 147
sperren 141, 162, 164
Überblick 159
vollständiger Name 141
wiederherstellen 164
Zertifikat 141
Zusatzeigenschaft zuweisen 151
Notes Client Version 16
Notes Domäne 134
bearbeiten 135
Berichte 230
ID-Vault nutzen 135
Kategorien festlegen 137
Kontendefinition 135
Zielsystemverantwortliche 135
Notes Gruppe 165
Administrator festlegen 173
Administratoren 176
administrierbare Dokumente 173
ausschließen 109

Ausschlussliste bearbeiten 180
bearbeiten 166
Benutzerkonto zuweisen 99, 107
Dokumentenbesitz 171
dynamische Gruppe 166, 179
Anzahl der Mitglieder 179
Ausschlussliste bearbeiten 179
Einschlussliste bearbeiten 179
Mitglieder berechnen 179
Eigentümer 175
Eigentümer festlegen 171
Einschlussliste bearbeiten 182
erstellen 166
Erweiterungsgruppe 179
Gruppenmitgliedschaft 107, 170
Kategorie 111
Kategorie zuordnen 166
löschen 183
Mail-In-Datenbank zuweisen 168
Risikoindex 166
Server zuweisen 169, 180
Sperrgruppe 166, 177
Anzahl der Mitglieder 177
über IT Shop bestellen 166
Überblicksformular 177
Vererbung über Kategorien 137
Vererbung über Rollen 99
wirksam 109
Zusatzeigenschaft zuweisen 176
Notes Server
Administrator 209
Administrator mit Leseberechtigung 213
Administratoren 208, 210
Administratorzugriff 208
Agenten ausführen 226-228
Ausschlussliste 229
bearbeiten 202
Benutzerkonto zuweisen 206
Datenbankadministrator 211
Durchgangsserver 204, 221, 224-225
Durchgangsziel 222, 225
dynamische Gruppe 229
Eigentümer 207
einrichten 201
Einschlussliste 229
Gruppe zuweisen 205
ID-Vault-Server 203
Kontakt 204
löschen 230
Mailserver 204, 206
Remotekonsolenadministrator 212
Replikation 220
Routing 221
Schablonen erstellen 218
Sicherheit 205
Stammdaten 203
Standort 204
Systemadministrator 214-215
Überblicksformular 230
Vollzugriffadministrator 209
Wählverbindung 224
Zielserver 225
Zugriff einschränken 216-217
Zugriff gewähren 216
Zugriff verweigern 217
Notes Serverdokument
Administrator 208
Eigentümer 207

Notes.INI 23

O

Objekt
- ausstehend 54
- publizieren 54
- sofort löschen 54

Offline-Modus 59

P

Person
- Benutzerkonto zuweisen 90
- deaktivieren 162
- Gruppenidenität 95
- Hauptidentität 94
- persönliche Administratoridentität 94
- primäre Identität 95

Personenzuordnung
- entfernen 87
- manuell 87
- Suchkriterium 86

Persönliche Administratoridentität 94
Postfachdatei 145
- erzeugen 47
- Größe beschränken 147
- logische Größe 147
- physische Größe 147

Projektvorlage 249
Protokolldatei 57
Provisionierung
- Mitgliederliste 42

Pseudo-Person 95

R

Revision zurücksetzen 57
Revisionsfilter 41
Richtlinie 190
- Administratoren 194
- Eigentümer 193
- Notes Benutzerkonten zuweisen 192
- Notes Gruppen zuweisen 192

Richtlinieneinstellung 192

S

Schablone 189
Schema
- aktualisieren 40
- Änderungen 40
- komprimieren 40

Server
- Administrator 211-215
- Administrator festlegen 173
- Datenbanken erstellen 218
- Eigentümer festlegen 171
- Not access server 162, 177

Serverberechtigung 216
Serverdokument
- Administrator festlegen 173

Serverfunktion
- Gateway Server 241

Serverzugriff 216
Sperrgruppe 177
Standardbenutzerkonto 92
Startinformation zurücksetzen 57
Startkonfiguration 38

Synchronisation
Ablauf 11
Basisobjekt
erstellen 37
Benutzer 18
Berechtigungen 18
beschleunigen 41
konfigurieren 31
nur Änderungen 41
Scope 35
simulieren 57
starten 31, 50
Synchronisationsprojekt
erstellen 31
Variable 35
Variablenset 37
Verbindungsparameter 31, 35, 37
verhindern 52
verschiedene Domänen 37
Voraussetzungen 16
Workflow 31, 36
Zeitplan 50
Synchronisationsanalysebericht 57
Synchronisationskonfiguration
anpassen 35-37
Synchronisationsprojekt
bearbeiten 138
deaktivieren 52
erstellen 31
Projektvorlage 249
Synchronisationsprotokoll 51, 57
Synchronisationsrichtung
In das Zielsystem 31, 36
In den One Identity Manager 31
Synchronisationsserver 20
für Domino 237
Serverfunktion 241
Synchronisationsworkflow
erstellen 31, 36
Systemverbindung
aktives Variablenset 39
ändern 37

V

Variablenset 38
aktiv 39
Verbindungsparameter umwandeln 38
Vererbung
Kategorie 111

Z

Zeitplan 50
deaktivieren 52
Zertifikat 184
Ablaufdatum 185
Administrator 187
Administrator festlegen 173
bearbeiten 184
CA-Datenbank 185
Eigentümer 186
Eigentümer festlegen 171
ID-Datei 185, 188
Überblicksformular 188
übernehmen 23
Zertifikatsanforderung 189
Zertifikatstyp 185
Zertifizierer
Kontaktdaten 186

Zielsystem
nicht verfügbar 59
Zielsystemabgleich 54
Zielsystemverantwortlicher
für Domino-Umgebung 242
Zusatzeigenschaft
Notes Benutzerkonto 151
Notes Gruppe 176