



## One Identity Manager 9.2

# Administrationshandbuch für die Anbindung einer SharePoint- Umgebung

**Copyright 2023 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](http://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 SharePoint-Umgebung  
Aktualisiert - 29. September 2023, 05:11 Uhr

Die aktuellsten Versionen der Produktdokumentation finden Sie unter [One Identity Manager Dokumentation](#).

# Inhalt

<b>Verwalten einer SharePoint Umgebung</b>	<b>8</b>
Architekturüberblick	9
One Identity Manager Benutzer für die Verwaltung einer SharePoint-Umgebung	10
Forderungsbasierte Authentifizierung	12
<b>Einrichten der Synchronisation mit einer SharePoint Farm</b>	<b>14</b>
Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Farm	15
Einrichten des Synchronisationsservers	16
Erstellen eines Synchronisationsprojekts für die initiale Synchronisation einer SharePoint Farm	21
Besonderheiten bei der Synchronisation zulässiger Berechtigungen	28
Synchronisationsergebnisse anzeigen	29
Anpassen einer Synchronisationskonfiguration	30
Synchronisation in die SharePoint-Umgebung konfigurieren	31
Synchronisation verschiedener SharePoint Farmen konfigurieren	32
Einstellungen der Systemverbindung zur SharePoint Farm ändern	33
Verbindungsparameter im Variablenset bearbeiten	33
Eigenschaften der Zielsystemverbindung bearbeiten	35
Schema aktualisieren	35
Beschleunigung der Synchronisation durch Revisionsfilterung	37
Nachbehandlung ausstehender Objekte	37
Provisionierung von Mitgliedschaften konfigurieren	39
Einzelobjektsynchronisation konfigurieren	41
Beschleunigung der Provisionierung und Einzelobjektsynchronisation	42
Unterstützung bei der Analyse von Synchronisationsproblemen	43
Deaktivieren der Synchronisation	44
Einzelobjekte synchronisieren	45
Datenfehler bei der Synchronisation ignorieren	46
Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus)	47
<b>Basisdaten für die Verwaltung einer SharePoint-Umgebung</b>	<b>49</b>
Authentifizierungsmodi	51
Präfixe	52

Zonen und alternative URLs .....	52
SharePoint Webvorlagen .....	53
SharePoint Berechtigungen .....	53
SharePoint Kontingente .....	54
SharePoint Sprachen .....	54
Bearbeiten eines Servers .....	54
Stammdaten eines Jobservers .....	55
Festlegen der Serverfunktionen .....	58
Zielsystemverantwortliche .....	60
Einrichten von Kontendefinitionen .....	62
Erstellen einer Kontendefinition .....	63
Stammdaten einer Kontendefinition .....	64
Erstellen der Automatisierungsgrade .....	67
Stammdaten eines Automatisierungsgrades .....	68
Erstellen einer Abbildungsvorschrift für IT Betriebsdaten .....	70
Erfassen der IT Betriebsdaten .....	71
IT Betriebsdaten ändern .....	72
Zuweisen der Kontendefinition an Identitäten .....	73
Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen .....	75
Kontendefinition an Geschäftsrollen zuweisen .....	75
Kontendefinition an alle Identitäten zuweisen .....	76
Kontendefinition direkt an Identitäten zuweisen .....	76
Kontendefinition an Systemrollen zuweisen .....	77
Kontendefinition in den IT Shop aufnehmen .....	77
Zuweisen der Kontendefinition an ein Zielsystem .....	80
Löschen einer Kontendefinition .....	80
<b>SharePoint Farmen .....</b>	<b>83</b>
Allgemeine Stammdaten einer SharePoint Farm .....	83
Synchronisationsprojekt bearbeiten .....	84
<b>SharePoint Webanwendungen .....</b>	<b>86</b>
<b>SharePoint Websitesammlungen und Websites .....</b>	<b>87</b>
SharePoint Websitesammlungen .....	87
Allgemeine Stammdaten einer Websitesammlung .....	88
Festlegen der Kategorien für die Vererbung von SharePoint Gruppen .....	89

SharePoint Websites .....	90
Allgemeine Stammdaten einer Website .....	90
Adressdaten einer Website .....	91
Designinformationen einer Website .....	92
Zusätzliche Aufgaben zur Verwaltung von Websites .....	93
Vererbung von Berechtigungen an untergeordnete Websites .....	93
Einrichten von SharePoint Websitesammlungen und Websites .....	94
<b>SharePoint Benutzerkonten .....</b>	<b>96</b>
Unterstützte Typen von Benutzerkonten .....	98
Erfassen der Stammdaten für SharePoint Benutzerkonten .....	102
Stammdaten eines gruppenauthentifizierten Benutzerkontos .....	103
Stammdaten eines benutzerauthentifizierten Benutzerkontos .....	107
Zusätzliche Aufgaben zur Verwaltung von SharePoint Benutzerkonten .....	113
Überblick über das SharePoint Benutzerkonto .....	113
SharePoint Gruppen direkt an ein SharePoint Benutzerkonto zuweisen .....	113
SharePoint Rollen direkt an ein Benutzerkonto zuweisen .....	114
Zusatzeigenschaften zuweisen .....	115
Unternehmensspezifische Authentifizierungsmodi nutzen .....	116
Automatische Zuordnung von Identitäten zu SharePoint Benutzerkonten .....	116
Bearbeiten der Suchkriterien für die automatische Identitätenzuordnung .....	118
Löschen und Wiederherstellen von SharePoint Benutzerkonten .....	120
<b>SharePoint Rollen und Gruppen .....</b>	<b>123</b>
SharePoint Gruppen .....	125
Erfassen der Stammdaten für SharePoint Gruppen .....	126
SharePoint Gruppen an SharePoint Benutzerkonten zuweisen .....	128
SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen .....	128
SharePoint Gruppen an Geschäftsrollen zuweisen .....	130
SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen .....	131
SharePoint Rollen an SharePoint Gruppen zuweisen .....	132
SharePoint Gruppen in Systemrollen aufnehmen .....	132
SharePoint Gruppen in den IT Shop aufnehmen .....	133
SharePoint Gruppen automatisch in den IT Shop aufnehmen .....	135
Zusätzliche Aufgaben für die Verwaltung von SharePoint Gruppen .....	137
Überblick über die SharePoint Gruppe .....	137

Wirksamkeit von Gruppenmitgliedschaften .....	137
Vererbung von SharePoint Gruppen anhand von Kategorien .....	140
Zusatzeigenschaften an SharePoint Gruppen zuweisen .....	142
Löschen von SharePoint Gruppen .....	142
Standardlösungen für die Bestellung von SharePoint Gruppen .....	143
Anlegen von SharePoint Gruppen .....	143
SharePoint Gruppenmitgliedschaften bestellen .....	144
SharePoint Rollen und Berechtigungsstufen .....	144
Erfassen der Stammdaten für SharePoint Berechtigungsstufen .....	145
Zusätzliche Aufgaben für die Verwaltung von SharePoint Berechtigungsstufen .....	146
Überblick über die SharePoint Berechtigungsstufe .....	146
Berechtigungen zuweisen .....	146
Besonderheiten bei der Synchronisation zulässiger Berechtigungen .....	147
Erfassen der Stammdaten für SharePoint Rollen .....	147
SharePoint Rollen an SharePoint Benutzerkonten zuweisen .....	149
SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen .....	150
SharePoint Rollen an Geschäftsrollen zuweisen .....	151
SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen .....	152
SharePoint Gruppen an SharePoint Rollen zuweisen .....	153
SharePoint Rollen in Systemrollen aufnehmen .....	153
SharePoint Rollen in den IT Shop aufnehmen .....	154
Zusätzliche Aufgaben für die Verwaltung von SharePoint Rollen .....	156
Überblick über die SharePoint Rolle .....	156
Wirksamkeit von SharePoint Rollen .....	156
Zusatzeigenschaften an SharePoint Rollen zuweisen .....	157
Löschen von SharePoint Rollen und Berechtigungsstufen .....	158
<b>Berechtigungen für SharePoint Webanwendungen .....</b>	<b>159</b>
SharePoint Berechtigungsrichtlinien .....	160
SharePoint Benutzerrichtlinien .....	160
<b>Berichte über SharePoint Objekte .....</b>	<b>163</b>
Übersicht aller Zuweisungen .....	165
<b>Anhang: Konfigurationsparameter für die Verwaltung einer SharePoint-Umgebung .....</b>	<b>167</b>
<b>Anhang: Standardprojektvorlage für SharePoint .....</b>	<b>169</b>

<b>Über uns</b> .....	<b>171</b>
Kontaktieren Sie uns .....	171
Technische Supportressourcen .....	171
<b>Index</b> .....	<b>172</b>

# Verwalten einer SharePoint Umgebung

Im One Identity Manager können die Komponenten und Zugriffsrechte von SharePoint 2013, SharePoint 2016, SharePoint 2019 und SharePoint Server Subscription Edition Umgebungen abgebildet werden. Ziel dieser Abbildung ist es, den Mitarbeitern eines Unternehmens Zugriffsrechte auf die Websites einer SharePoint-Umgebung zu gewähren. Für diese Abbildung werden Informationen über folgende Komponenten der SharePoint Umgebung in die One Identity Manager-Datenbank eingelesen.

- die Farm als oberste Ebene der logischen Architektur der SharePoint-Umgebung  
Die SharePoint Farm wird als Basisobjekt für die Synchronisation in der One Identity Manager-Datenbank eingerichtet.
- alle innerhalb der Farm eingerichteten Webanwendungen mit ihren Benutzerrichtlinien und zulässigen Berechtigungen
- alle Websitesammlungen dieser Webanwendungen mit ihren Benutzerkonten und Gruppen
- alle Websites, die innerhalb der Websitesammlungen in einer hierarchischen Struktur angelegt sind (jedoch nicht deren Inhalt)
- alle Berechtigungsstufen und SharePoint Rollen, welche die Berechtigungen auf die einzelnen Websites definieren

SharePoint Rollen, Gruppen und Benutzerkonten werden im Kontext der SharePoint-Komponenten abgebildet, für die sie eingerichtet sind. Über diese Objekte werden im One Identity Manager den SharePoint Benutzern die Zugriffsrechte auf die verschiedenen Websites zur Verfügung gestellt. Dafür können Sie die unterschiedlichen Mechanismen des One Identity Managers für die Verbindung der Identitäten mit ihren SharePoint Benutzerkonten nutzen. Es werden folgende Objekte provisioniert:

- SharePoint Benutzerkonten und ihre Beziehungen zu SharePoint Rollen und Gruppen
- SharePoint Gruppen und ihre Zuordnungen zu Benutzerkonten und Rollen
- SharePoint Rollen und ihre Berechtigungen auf Websites

Für die Anmeldung am SharePoint Server unterstützt der One Identity Manager sowohl die klassische Windows-Authentifizierung als auch die forderungsbasierte Authentifizierung. Jedem SharePoint Benutzerkonto, das sich über die klassische Windows-Authentifizierung



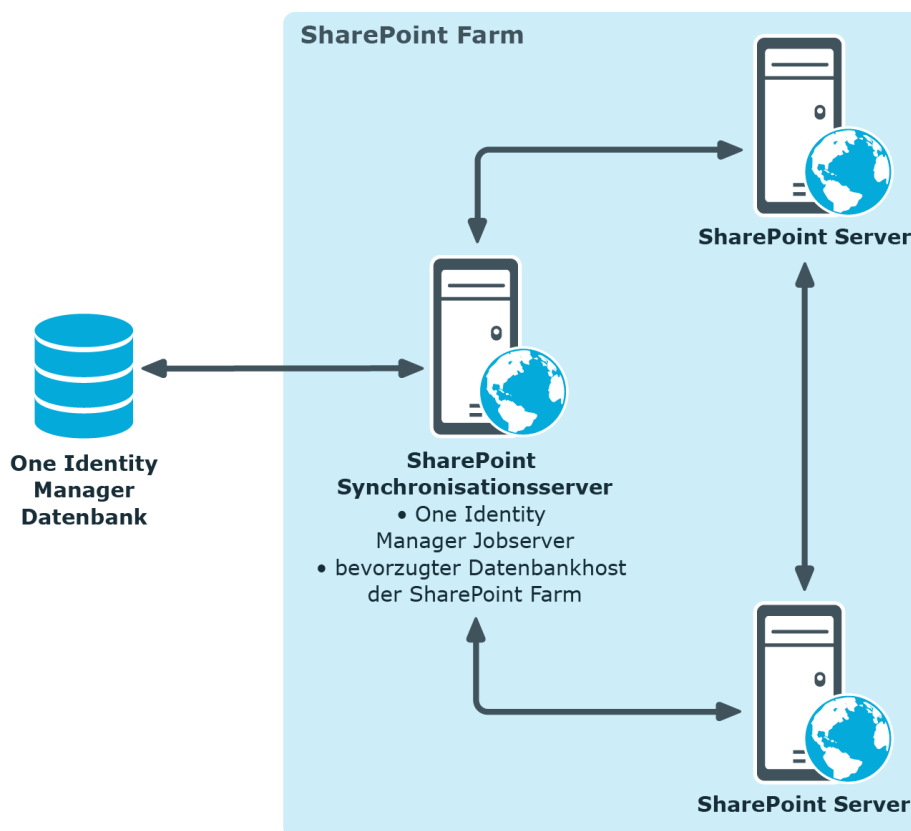
anmelden kann, ist im One Identity Manager ein Active Directory oder LDAP Benutzerkonto bzw. eine Active Directory oder LDAP Gruppe zugeordnet. Voraussetzung dafür ist, dass die zugehörige Active Directory bzw. LDAP-Umgebung ebenfalls in der One Identity Manager-Datenbank abgebildet werden. Informationen über die in der SharePoint-Umgebung genutzten Authentifizierungssysteme können im One Identity Manager gepflegt werden.

Zu jedem SharePoint Benutzerkonto, das mit einem Active Directory oder LDAP Benutzerkonto verbunden ist, kann zusätzlich eine in der One Identity Manager-Datenbank hinterlegte Identität zugeordnet werden. Damit ist es möglich, die Mitgliedschaften von Identitäten in SharePoint Rollen und Gruppen zu pflegen. Über die Zuordnung von SharePoint Rollen und Gruppen zu den Unternehmensstrukturen können SharePoint Berechtigungen an die Identitäten vererbt werden. Außerdem ist es möglich, Berechtigungen über den IT Shop zu bestellen. Über Complianceregeln können die einer Identität zugewiesenen Berechtigungen überwacht werden.

## Architekturüberblick

Der SharePoint-Konnektor wird für die Synchronisation und Provisionierung der SharePoint-Umgebung eingesetzt. Der Konnektor kommuniziert direkt mit den SharePoint Servern einer SharePoint Farm.

**Abbildung 1: Kommunikationsweg des Konnektors mit der SharePoint-Umgebung**



Für die Synchronisation und Provisionierung müssen auf einem beliebigen Server der SharePoint Farm der One Identity Manager Service, der SharePoint Konnektor und der Synchronization Editor installiert sein. Dieser Server wird im Weiteren als Synchronisationsserver bezeichnet. 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.

## Detaillierte Informationen zum Thema

- [Einrichten des Synchronisationsservers](#) auf Seite 16

# One Identity Manager Benutzer für die Verwaltung einer SharePoint-Umgebung

In die Verwaltung einer SharePoint-Umgebung mit dem One Identity Manager sind folgende Benutzer eingebunden.

**Tabelle 1: Benutzer**

Benutzer	Aufgaben
Zielsystemadministratoren	<p>Die Zielsystemadministratoren müssen der Anwendungsrolle <b>Zielsysteme   Administratoren</b> zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"><li>• Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen.</li><li>• Legen die Zielsystemverantwortlichen fest.</li><li>• Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein.</li><li>• Legen fest, welche Anwendungsrollen für Zielsystemverantwortliche sich ausschließen.</li><li>• Berechtigen weitere Identitäten als Zielsystemadministratoren.</li><li>• Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.</li></ul>
Zielsystemverantwortliche	<p>Die Zielsystemverantwortlichen müssen der Anwendungsrolle <b>Zielsysteme   SharePoint</b> oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p>

## Benutzer

## Aufgaben

Benutzer mit dieser Anwendungsrolle:

- Übernehmen die administrativen Aufgaben für das Zielsystem.
- Erzeugen, ändern oder löschen die Zielsystemobjekte.
- Bearbeiten Kennwortrichtlinien für das Zielsystem.
- Bereiten Systemberechtigungen zur Aufnahme in den IT Shop vor.
- Können Identitäten anlegen, die nicht den Identitätstyp **Primäre Identität** haben.
- 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 Identitäten 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.

Benutzer	Aufgaben
Administratoren für den IT Shop	<p>Die Administratoren müssen der Anwendungsrolle <b>Request &amp; Fulfillment   IT Shop   Administratoren</b> zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> <li>• Weisen Systemberechtigungen an IT Shop-Strukturen zu.</li> </ul>
Produkteigner für den IT Shop	<p>Die Produkteigner müssen der Anwendungsrolle <b>Request &amp; Fulfillment   IT Shop   Produkteigner</b> oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> <li>• Entscheiden über Bestellungen.</li> <li>• Bearbeiten die Leistungspositionen und Servicekategorien, für die sie verantwortlich sind.</li> </ul>
Administratoren für Organisationen	<p>Die Administratoren müssen der Anwendungsrolle <b>Identity Management   Organisationen   Administratoren</b> zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> <li>• Weisen Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zu.</li> </ul>
Administratoren für Geschäftsrollen	<p>Die Administratoren müssen der Anwendungsrolle <b>Identity Management   Geschäftsrollen   Administratoren</b> zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> <li>• Weisen Systemberechtigungen an Geschäftsrollen zu.</li> </ul>

## Forderungsbasierte Authentifizierung

Für die Anmeldung am SharePoint Server unterstützt der One Identity Manager sowohl die forderungsbasierte Authentifizierung als auch die klassische Windows-Authentifizierung. Dafür werden in der Datenbank Informationen über die verwendeten SharePoint Provider und Authentifizierungsmodi hinterlegt. Die vorhandenen SharePoint Provider zur forderungsbasierten Authentifizierung müssen durch die Synchronisation in die Datenbank eingelesen werden. Für jede Webanwendung sind die zugelassenen Provider hinterlegt.

An jedem Benutzerkonto ist hinterlegt, mit welchem Authentifizierungsmodus sich der Benutzer mit diesem Benutzerkonto anmeldet. Der standardmäßig zugeordnete Authentifizierungsmodus ist abhängig davon, ob die forderungsbasierte Authentifizierung an der zugehörigen Webanwendung zugelassen ist.

Der Authentifizierungsmodus wird benötigt, um Benutzerkonten im One Identity Manager anzulegen. Der Anmeldename von Benutzerkonten für die forderungsbasierte Authentifizierung enthält ein Präfix, das vom genutzten Authentifizierungsmodus abhängig ist. Diese Präfixe müssen an den Authentifizierungsmodi gepflegt werden.

## Verwandte Themen

- [Authentifizierungsmodi](#) auf Seite 51

# Einrichten der Synchronisation mit einer SharePoint Farm

## **Um die Objekte einer SharePoint Umgebung initial in die One Identity Manager-Datenbank einzulesen**

1. Stellen Sie in der SharePoint-Umgebung ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Die One Identity Manager Bestandteile für die Verwaltung von SharePoint-Umgebungen sind verfügbar, wenn der Konfigurationsparameter **TargetSystem | SharePoint** aktiviert ist.

Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.

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

Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.

3. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
4. Synchronisieren Sie die Active Directory oder LDAP Umgebung, auf der die SharePoint Umgebung aufgesetzt ist.

Ausführliche Informationen zur Synchronisation einer Active Directory Umgebung finden Sie im One Identity Manager Administrationshandbuch für die Anbindung einer Active Directory-Umgebung. Ausführliche Informationen zur Synchronisation einer LDAP Umgebung finden Sie im One Identity Manager Administrationshandbuch für die Anbindung einer LDAP-Umgebung.

**WICHTIG:** Um inkonsistente Daten zu vermeiden, synchronisieren Sie immer zuerst die Active Directory oder LDAP Umgebung, auf der die SharePoint Umgebung aufgesetzt ist. Erst wenn diese Synchronisation erfolgreich

abgeschlossen ist, starten Sie die Synchronisation der SharePoint Farm.

Wenn das nicht sichergestellt werden kann, definieren Sie unternehmensspezifische Prozesse, um SharePoint Benutzerkonten und Benutzerrichtlinien mit den zugehörigen Authentifizierungsobjekten zu verbinden.

5. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

**HINWEIS:** Um ein Synchronisationsprojekt zu erstellen oder zu bearbeiten, starten Sie den Synchronization Editor auf dem Synchronisationsserver oder einem Remoteverbindungsserver. Ausführliche Informationen zur Einrichtung einer Remoteverbindung finden Sie im One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation.

## Detaillierte Informationen zum Thema

- [Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Farm](#) auf Seite 15
- [Einrichten des Synchronisationsservers](#) auf Seite 16
- [Erstellen eines Synchronisationsprojekts für die initiale Synchronisation einer SharePoint Farm](#) auf Seite 21
- [Konfigurationsparameter für die Verwaltung einer SharePoint-Umgebung](#) auf Seite 167

# Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Farm

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

**Tabelle 2: Benutzer für die Synchronisation**

Benutzer	Berechtigungen
Benutzer für den Zugriff auf die SharePoint Farm	Für die Anmeldung an der SharePoint Farm während der Synchronisation nutzt der Konnektor das Serverfarmkonto (Farm Account). Stellen Sie die Anmeldedaten des Serverfarmkontos bereit.  Es kann keine sinnvolle Minimalkonfiguration empfohlen werden, die sich effektiv in ihren Berechtigungen von dem Serverfarmkonto unterscheidet. Die Mitgliedschaft in der Gruppe "Farm Administrators" genügt <b>nicht</b> .
Benutzerkonto des	Als Benutzerkonto für den

Benutzer	Berechtigungen
One Identity Manager Service	<p>One Identity Manager Service muss das Serverfarmkonto der SharePoint Farm genutzt werden.</p> <p>Das Benutzerkonto für den One Identity Manager Service benötigt zusätzlich die Benutzerrechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Verzeichnisse und Dateien anlegen und bearbeiten.</p> <p>Das Benutzerkonto muss der Gruppe <b>Domänen-Benutzer</b> angehören.</p> <p>Das Benutzerkonto benötigt das erweiterte Benutzerrecht <b>Anmelden als Dienst</b>.</p> <p>Das Benutzerkonto benötigt Berechtigungen für den internen Webservice.</p> <p><b>HINWEIS:</b> Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (<b>NT Authority\NetworkService</b>) laufen, so können Sie die Berechtigungen für den internen Webservice über folgenden Kommandozeilenauftrag vergeben:</p> <pre>netsh http add urlacl url=http://&lt;IP-Adresse&gt;:&lt;Portnummer&gt;/ user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis.</p> <p>In der Standardinstallation wird der One Identity Manager installiert unter:</p> <ul style="list-style-type: none"> <li>• %ProgramFiles(x86)%\One Identity (auf 32-Bit Betriebssystemen)</li> <li>• %ProgramFiles%\One Identity (auf 64-Bit Betriebssystemen)</li> </ul>
Benutzer für den Zugriff auf die One Identity Manager-Datenbank	<p>Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer <b>Synchronization</b> bereitgestellt.</p>

## Einrichten des Synchronisationsservers

Für die Synchronisation mit einer SharePoint-Umgebung muss ein Synchronisationsserver bereitgestellt werden. Sie können dafür einen beliebigen SharePoint Server der SharePoint



Farm nutzen. Auf dem Synchronisationsserver muss die nachfolgend genannte Software installiert sein.

**HINWEIS:** Ein und derselbe Synchronisationsserver sollte niemals parallel mehrere Synchronisationen ausführen. Verschiedene Synchronisationsserver sollten niemals parallel Synchronisationen für ein und dieselbe SharePoint Farm ausführen.

Wenn Sie die Synchronisation einer SharePoint Farm auf verschiedene Startkonfigurationen aufteilen, stellen Sie sicher, dass diese Startkonfigurationen nacheinander ausgeführt werden. Ausführliche Informationen zum Einrichten von Startkonfigurationen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*. Weitere Informationen finden Sie unter [Anpassen einer Synchronisationskonfiguration](#) auf Seite 30.

### **Um eine SharePoint 2013, 2016, 2019 oder Subscription Edition Umgebung zu synchronisieren**

- Windows Server 2008 R2 oder Windows Server 2012
- Microsoft SharePoint Server 2013, 2016, 2019 beziehungsweise Subscription Edition
- Microsoft .NET Framework Version 4.8 oder höher

**HINWEIS:** Beachten Sie die Empfehlungen des Zielsystemherstellers.

- One Identity Manager Service, SharePoint 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 | Job Server | SharePoint**.

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 einen Jobserver einzurichten, führen Sie folgende Schritte aus.

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

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

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

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

Für die Remote-Installation des One Identity Manager Service stellen Sie eine administrative Arbeitsstation bereit, auf der die One Identity Manager-Komponenten installiert sind. Für eine lokale Installation stellen Sie sicher, dass die One Identity Manager-Komponenten auf dem Server installiert sind. Ausführliche Informationen zur Installation der One Identity Manager-Komponenten finden Sie im *One Identity Manager Installationshandbuch*.

2. Wenn Sie mit einer verschlüsselten One Identity Manager-Datenbank arbeiten, geben Sie dem One Identity Manager Service den Datenbankschlüssel bekannt. Ausführliche Informationen zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank finden Sie im *One Identity Manager Installationshandbuch*.
3. Für die Generierung von Prozessen für die Jobserver werden der Provider, Verbindungsparameter und die Authentifizierungsdaten benötigt. Diese Informationen werden im Standardfall aus den Verbindungsdaten der Datenbank ermittelt. Arbeitet der Jobserver über einen Anwendungsserver müssen Sie zusätzliche Verbindungsinformationen im Designer konfigurieren. Ausführliche Informationen zum Erfassen der Verbindungsinformationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

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

1. Starten Sie das Programm Server Installer.

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

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

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

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

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

- ODER -

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

- b. Bearbeiten Sie folgende Informationen für den Jobserver.

- **Server:** Bezeichnung des Jobservers.
- **Queue:** Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder Jobserver innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert.

Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.

- **Vollständiger Servername:** Vollständiger Servername gemäß DNS-Syntax.

Syntax:

<Name des Servers>.<Vollqualifizierter Domänenname>

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

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

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

Für eine direkte Verbindung zu Datenbank:

- a. Wählen Sie in der Modulliste **Prozessabholung > sqlprovider**.
- b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
- c. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
- d. Klicken Sie **OK**.

Für eine Verbindung zum Anwendungsserver:

- a. Wählen Sie in der Modulliste den Eintrag **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen**.
- b. Wählen Sie **AppServerJobProvider** und klicken Sie **OK**.
- c. Wählen Sie in der Modulliste **Prozessabholung > AppServerJobProvider**.
- d. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
- e. Erfassen Sie die Adresse (URL) zum Anwendungsserver und klicken Sie **OK**.
- f. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
- g. Wählen Sie unter **Authentifizierungsverfahren** das Authentifizierungsmodul für die Anmeldung. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager-Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur*

### *Autorisierung und Authentifizierung.*

h. Klicken Sie **OK**.

7. Zur Konfiguration der Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.
10. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
  - **Computer:** Wählen Sie den Server über die Auswahlliste oder erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.

Um die Installation lokal auszuführen, wählen Sie in der Auswahlliste den Eintrag **<lokale Installation>**.
  - **Dienstkonto:** Erfassen Sie die Angaben zum Benutzerkonto unter dem der One Identity Manager Service läuft. Erfassen Sie das Benutzerkonto, das Kennwort zum Benutzerkonto und die Kennwortwiederholung.

Als Benutzerkonto für den One Identity Manager Service muss das Serverfarmkonto der SharePoint Farm genutzt werden.

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

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

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

Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.
12. Auf der letzten Seite des Server Installer klicken Sie **Fertig**.

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

# Erstellen eines Synchronisationsprojekts für die initiale Synchronisation einer SharePoint Farm

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

Ein Synchronisationsprojekt ist die Zusammenstellung aller Informationen, die für die Synchronisation der One Identity Manager-Datenbank mit einem Zielsystem benötigt werden. Dazu gehören die Verbindungsinformationen zum Zielsystem, Schematypen und -eigenschaften, Mappings und Synchronisationsworkflows.

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

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

**Tabelle 3: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes**

Angaben	Erläuterungen
SharePoint Version	Der One Identity Manager unterstützt die Synchronisation mit den SharePoint Versionen 2013, 2016, 2019 und mit SharePoint Server Subscription Edition.
Benutzername und Kennwort zur Anmeldung an der SharePoint Farm	Um auf die SharePoint Objekte zugreifen zu können, meldet sich der Konnektor mit dem Serverfarmkonto an der SharePoint Farm an. Es werden der Benutzername und das Kennwort des Serverfarmkontos benötigt. Weitere Informationen finden Sie unter <a href="#">Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Farm</a> auf Seite 15.
Domäne	Domäne des Serverfarmkontos.
Synchronisationsserver	Vom Synchronisationsserver werden alle Aktionen des One Identity Manager Service gegen die Zielsystemumgebung ausgeführt. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet.  Installierte Komponenten:

Angaben	Erläuterungen
	<ul style="list-style-type: none"> <li>• SharePoint Server</li> <li>• One Identity Manager Service (gestartet)</li> <li>• Synchronization Editor</li> <li>• SharePoint Konnektor</li> </ul> <p>Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt.</p> <p>Weitere Informationen finden Sie unter <a href="#">Einrichten des Synchronisationsservers</a> auf Seite 16.</p>
Remoteverbindungsserver	<p>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 Synchronisationsserver gestartet werden kann, kann eine Remoteverbindung eingerichtet werden.</p> <p><b>Um eine Remoteverbindung zu nutzen</b></p> <ol style="list-style-type: none"> <li>1. Stellen Sie eine Arbeitsstation bereit, auf der der Synchronization Editor installiert ist.</li> <li>2. Installieren Sie das <b>RemoteConnectPlugin</b> auf dem Synchronisationsserver.</li> </ol> <p>Damit übernimmt der Synchronisationsserver gleichzeitig die Funktion des Remoteverbindungservers.</p> <p>Der Remoteverbindungsserver und die Arbeitsstation müssen in der selben Active Directory Domäne stehen.</p> <p>Konfiguration des Remoteverbindungservers:</p> <ul style="list-style-type: none"> <li>• One Identity Manager Service ist gestartet</li> <li>• <b>RemoteConnectPlugin</b> ist installiert</li> <li>• SharePoint Konnektor ist installiert</li> <li>• Zielsystemspezifische Komponenten sind installiert</li> </ul> <p>Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird</p>

Angaben	Erläuterungen
	<p>der Name des Jobserver benötigt.</p> <p>Ausführliche Informationen zum Herstellen einer Remoteverbindung finden Sie im <i>One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation</i>.</p>
Verbindungsdaten zur One Identity Manager-Datenbank	<ul style="list-style-type: none"> <li>• Datenbankserver</li> <li>• Name der Datenbank</li> <li>• SQL Server-Anmeldung und Kennwort</li> <li>• Angabe, ob integrierte Windows-Authentifizierung verwendet wird</li> </ul> <p>Die Verwendung der integrierten Windows-Authentifizierung wird nicht empfohlen. Sollten Sie das Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.</p>

Beim Erstellen eines Synchronisationsprojekts unterstützt Sie ein Assistent. Dieser Assistent führt Sie durch alle Schritte, die zum initialen Einrichten der Synchronisation mit einem Zielsystem erforderlich sind. Wenn Sie alle erforderlichen Angaben für einen Schritt erfasst haben, klicken Sie **Weiter**.

**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 SharePoint Farm einzurichten

1. Starten Sie das Launchpad auf dem Synchronisationsserver 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 SharePoint** und klicken Sie **Starten**.

Der Projektassistent des Synchronization Editors wird gestartet.

3. Auf der Startseite des Projektassistenten klicken Sie **Weiter**.

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

- Haben Sie das Launchpad auf dem Synchronisationsserver 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 Synchronisationsserver, über den die Verbindung hergestellt werden soll.

5. Im Systemverbindungsassistenten erfassen Sie die Verbindungsdaten zur SharePoint Farm. Sie können die Verbindung testen und die Verbindungsdaten speichern.
  - Erfassen Sie folgende Verbindungsdaten.

**Tabelle 4: Verbindungsdaten zur SharePoint Farm**

Eigenschaft	Beschreibung
SharePoint Version	Genutzte SharePoint Version. <ul style="list-style-type: none"> <li>• Für die Anbindung einer SharePoint Server Subscription Edition Umgebung wählen Sie <b>2019</b>.</li> </ul>
Domäne	Domäne des Serverfarmkontos.
Benutzername und Kennwort	Benutzername und Kennwort des Serverfarmkontos (Farm Account).  Dieses Benutzerkonto wird zur Synchronisation der SharePoint Objekte genutzt.

- Klicken Sie **Jetzt prüfen**, um die Verbindungsdaten zu prüfen.  
Der Synchronization Editor versucht sich an der SharePoint Farm anzumelden.
- Um die Verbindungsdaten zu speichern, aktivieren Sie **Verbindung auf dem Computer lokal speichern**. Diese können Sie bei der Einrichtung weiterer Synchronisationsprojekte nutzen.

6. 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.

7. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.




8. Auf der Seite **Zielsystemzugriff einschränken** legen Sie fest, wie der Systemzugriff erfolgen soll. Zur Auswahl stehen:

**Tabelle 5: Zielsystemzugriff festlegen**

Option	Bedeutung
Das Zielsystem soll nur eingelesen werden.	<p>Gibt an, ob nur ein Synchronisationsworkflow zum initialen Einlesen des Zielsystems in die One Identity Manager-Datenbank eingerichtet werden soll.</p> <p>Der Synchronisationsworkflow zeigt folgende Besonderheiten:</p> <ul style="list-style-type: none"><li>• Die Synchronisationsrichtung ist <b>In den One Identity Manager</b>.</li><li>• In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung <b>In den One Identity Manager</b> definiert.</li></ul>
Es sollen auch Änderungen im Zielsystem durchgeführt werden.	<p>Gibt an, ob zusätzlich zum Synchronisationsworkflow zum initialen Einlesen des Zielsystems ein Provisionierungsworkflow eingerichtet werden soll.</p> <p>Der Provisionierungsworkflow zeigt folgende Besonderheiten:</p> <ul style="list-style-type: none"><li>• Die Synchronisationsrichtung ist <b>In das Zielsystem</b>.</li><li>• In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung <b>In das Zielsystem</b> definiert.</li><li>• Synchronisationsschritte werden nur für solche Schemaklassen erstellt, deren Schematypen schreibbar sind.</li></ul>

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

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

- Klicken Sie , um einen neuen Jobserver anzulegen.
- Erfassen Sie die Bezeichnung des Jobservers und den vollständigen Servernamen gemäß DNS-Syntax.

**TIPP:** Sie können auch einen vorhandenen Jobserver zusätzlich als Synchronisationsserver für dieses Zielsystem einsetzen.

- Um einen Jobserver auszuwählen, klicken Sie .

Diesem Jobserver wird die passende Serverfunktion automatisch zugewiesen.

- 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.

10. 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.

### **Um den Inhalt des Synchronisationsprotokolls zu konfigurieren**

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

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

7. Klicken Sie **OK**.

### **Um regelmäßige Synchronisationen auszuführen**

1. Öffnen Sie 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**.

### **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**.

#### **HINWEIS:**

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

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

### **Um die Benutzerkonten über Kontendefinitionen zu verwalten**

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie der Websitesammlung 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 **SharePoint > Benutzerkonten (benutzerauthentifiziert) > Verbunden aber nicht konfiguriert > <Websitesammlung>**.

- b. Wählen Sie im Manager die Kategorie **SharePoint Online > Benutzerkonten (benutzerauthentifiziert) > Verbunden aber nicht konfiguriert > <Websitesammlung>**.
- c. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.
- d. Wählen Sie in der Auswahlliste **Kontendefinition** die Kontendefinition.
- e. Wählen Sie die Benutzerkonten, die die Kontendefinition erhalten sollen.
- f. Speichern Sie die Änderungen.

## Detaillierte Informationen zum Thema

- Weitere Informationen finden Sie im One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation.

## Verwandte Themen

- [Einrichten des Synchronisationsservers](#) auf Seite 16
- [Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Farm](#) auf Seite 15
- [Standardprojektvorlage für SharePoint](#) auf Seite 169
- [Einrichten von Kontendefinitionen](#) auf Seite 62
- [Automatische Zuordnung von Identitäten zu SharePoint Benutzerkonten](#) auf Seite 116

# Besonderheiten bei der Synchronisation zulässiger Berechtigungen

Zulässige Berechtigungen werden in der One Identity Manager-Datenbank in der Tabelle `SPSWebAppHasPermission` abgebildet; Zuweisungen von zulässigen Berechtigungen an Berechtigungsstufen werden in der Tabelle `SPSRoleHasSPSPPermission` abgebildet.

Wenn in der SharePoint-Umgebung eine Berechtigung aus der Liste der zulässigen Berechtigungen für eine Webanwendung entfernt wird, kann diese Berechtigung ab diesem Zeitpunkt keiner Berechtigungsstufe innerhalb der Webanwendung zugewiesen werden. Bereits bestehende Zuweisungen der Berechtigung zu einer Berechtigungsstufe bleiben erhalten, sind jedoch nicht wirksam. Bei der Synchronisation wird diese Berechtigung aus der Tabelle `SPSWebAppHasPermission` gelöscht. Bereits bestehende Zuweisungen der Berechtigung zu einer Berechtigungsstufe werden nicht geändert. Die unwirksamen Berechtigungen werden auf dem Übersichtformular der Berechtigungsstufen angezeigt.

## Verwandte Themen

- [SharePoint Rollen und Berechtigungsstufen](#) auf Seite 144

# 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.

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

## **Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen**

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

# Anpassen einer Synchronisationskonfiguration

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

Um die Datenbank und die SharePoint-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 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 Farmen eingerichtet werden. Hinterlegen Sie die Verbindungsparameter zur Anmeldung an den Farmen als Variablen.
- Um festzulegen, welche SharePoint 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.
- Wenn sich das One Identity Manager Schema oder das Zielsystemschemata geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.

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

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

One Identity Manager in diesem Fall verhalten soll.

- Stellen Sie über den Zeitplan sicher, dass die Startkonfigurationen nacheinander ausgeführt werden.
- Gruppieren Sie die Startkonfigurationen mit gleichem Startverhalten. Legen Sie als Startverhalten **Mit Fehler abbrechen** oder **Zurückstellen und warten** fest.

## Detaillierte Informationen zum Thema

- [Synchronisation in die SharePoint-Umgebung konfigurieren](#) auf Seite 31
- [Synchronisation verschiedener SharePoint Farmen konfigurieren](#) auf Seite 32
- [Schema aktualisieren](#) auf Seite 35
- [Einstellungen der Systemverbindung zur SharePoint Farm ändern](#) auf Seite 33
- One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation

# Synchronisation in die SharePoint-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 SharePoint Farm zu erstellen**

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.  
**TIPP:** Um ein bestehendes Synchronisationsprojekt anzupassen, können Sie den Synchronization Editor auf einem beliebigen Server starten. Für die Kommunikation mit den Servern der Farm richten Sie eine Remoteverbindung ein.
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.

## Detaillierte Informationen zum Thema

- [Synchronisation verschiedener SharePoint Farmen konfigurieren](#) auf Seite 32

# Synchronisation verschiedener SharePoint Farmen konfigurieren

## Voraussetzungen

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

## **Um ein Synchronisationsprojekt für die Synchronisation einer weiteren Farm anzupassen**

1. Installieren und konfigurieren Sie einen Synchronisationsserver für die weitere Farm. Geben Sie diesen Server im One Identity Manager als Jobserver bekannt.
2. Stellen Sie in der weiteren Farm ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
3. Synchronisieren Sie die Active Directory oder LDAP Umgebung, auf der die weitere Farm aufgesetzt ist.
4. Starten Sie den Synchronization Editor auf dem Synchronisationsserver der weiteren Farm und melden Sie sich an der One Identity Manager-Datenbank an.
5. Öffnen Sie das Synchronisationsprojekt.
6. Erstellen Sie für die weitere Farm ein neues Basisobjekt.
  - Verwenden Sie den Assistenten zur Anlage eines Basisobjektes.
  - Wählen Sie im Assistenten den SharePoint 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.

7. Passen Sie bei Bedarf weitere Komponenten der Synchronisationskonfiguration an.
8. Speichern Sie die Änderungen.
9. Führen Sie eine Konsistenzprüfung durch.

## Detaillierte Informationen zum Thema

- [Einrichten des Synchronisationsservers](#) auf Seite 16
- [Benutzer und Berechtigungen für die Synchronisation mit einer SharePoint Farm](#)



auf Seite 15

- [Synchronisation in die SharePoint-Umgebung konfigurieren](#) auf Seite 31

## Einstellungen der Systemverbindung zur SharePoint Farm 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 33
- [Eigenschaften der Zielsystemverbindung bearbeiten](#) auf Seite 35

## 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 SharePoint Farmen 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 35

# 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 33

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

### ***Um das Schema einer Systemverbindung zu aktualisieren***

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
  - ODER -
  - Wählen Sie die Kategorie **Konfiguration > One Identity Manager Verbindung**.
3. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Die Schemadaten werden neu geladen.

### ***Um ein Mapping zu bearbeiten***

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

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

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

# Beschleunigung der Synchronisation durch Revisionsfilterung

Die Synchronisation mit SharePoint unterstützt keine Revisionsfilterung.

## Nachbehandlung ausstehender Objekte

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

Ausstehende Objekte

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

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

Führen Sie dafür einen Zielsystemabgleich durch.

### **Um ausstehende Objekte nachzubearbeiten**

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

In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp **SharePoint** 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 Formularymbolleiste eins der folgenden Symbole, um die jeweilige Methode auszuführen.

**Tabelle 6: Methoden zur Behandlung ausstehender Objekte**

Symbol	Methode	Beschreibung
	Löschen	Das Objekt wird sofort in der One Identity Manager-Datenbank gelöscht. Eine Löschverzögerung wird nicht berücksichtigt.  Indirekte Mitgliedschaften können nicht gelöscht werden.
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung <b>Ausstehend</b> wird für das Objekt entfernt.  Es wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt.  Voraussetzungen: <ul style="list-style-type: none"> <li>• Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen.</li> <li>• Der Zielsystemkonnektor kann schreibend auf das Zielsystem zugreifen.</li> </ul>
	Zurücksetzen	Die Markierung <b>Ausstehend</b> wird für das Objekt entfernt.

**TIPP:** Wenn eine Methode wegen bestimmter Einschränkungen nicht ausgeführt werden kann, ist das jeweilige Symbol deaktiviert.

- Um Details zur Einschränkung anzuzeigen, klicken Sie in der Spalte **Einschränkungen** die Schaltfläche **Anzeigen**.
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 Formularymbolleiste das Symbol .

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

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

## **Provisionierung von Mitgliedschaften konfigurieren**

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

- Mitgliedschaften werden im Zielsystem in Form einer Liste als Eigenschaft eines Objekts gespeichert.  
Beispiel: Liste von Benutzerkonten in der Eigenschaft Users einer SharePoint Gruppe (SPGroup)
- 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 **SharePoint > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **SharePoint**.
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: SPSGroupHasSPSRLAsgn und SPSUserHasSPSRLAsgn


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 SPSUserHasSPSRLAsgn:

```
exists (select top 1 1 from SPSRLAsgn g
        where g.UID_SPSRLAsgn = i.UID_SPSRLAsgn
        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 **SharePoint > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **SharePoint**.
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\_SPSFarm).XObjectKey

8. Speichern Sie die Änderungen.

### **Verwandte Themen**

- [Einzelobjekte synchronisieren](#) auf Seite 45
- [Nachbehandlung ausstehender Objekte](#) auf Seite 37

## **Beschleunigung der Provisionierung und Einzelobjektsynchronisation**

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

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

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

### **Um die Lastverteilung zu konfigurieren**

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

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

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

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

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

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

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

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

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

### **Um den Synchronisationsserver ohne Lastverteilung zu nutzen**

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

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

### **Detaillierte Informationen zum Thema**

- [Bearbeiten eines Servers](#) auf Seite 54

## **Unterstützung bei der Analyse von Synchronisationsproblemen**

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

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

### ***Um den Synchronisationsanalysebericht zu erstellen***

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

Die Generierung des Berichts nimmt einige Zeit in Anspruch. Er wird in einem separaten Fenster angezeigt.

3. Drucken Sie den Bericht oder Speichern Sie ihn in einem der verschiedenen Ausgabeformate.

## **Deaktivieren der Synchronisation**

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

### ***Um regelmäßige Synchronisationen zu verhindern***

1. Öffnen Sie 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**.

## Detaillierte Informationen zum Thema

- Erstellen eines Synchronisationsprojekts für die initiale Synchronisation einer SharePoint Farm auf Seite 21
- Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) auf Seite 47

# 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 **SharePoint**.
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 SharePoint Benutzerkonten an SharePoint 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.

- [Einzelobjektsynchronisation konfigurieren](#) auf Seite 41

# 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 Synchronisationsserver 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**

- [Deaktivieren der Synchronisation](#) auf Seite 44



## Basisdaten für die Verwaltung einer SharePoint-Umgebung

Für die Verwaltung von SharePoint-Umgebungen im One Identity Manager sind folgende Basisdaten relevant.

- Konfigurationsparameter

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

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

Weitere Informationen finden Sie unter [Konfigurationsparameter für die Verwaltung einer SharePoint-Umgebung](#) auf Seite 167.

- Kontendefinitionen

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

Weitere Informationen finden Sie unter [Einrichten von Kontendefinitionen](#) auf Seite 62.

- Authentifizierungsmodi

Für die Anmeldung am SharePoint Server unterstützt der One Identity Manager sowohl die forderungsbasierte Authentifizierung als auch die klassische Windows-Authentifizierung. An den Webanwendungen und an den Benutzerkonten ist der verwendete Authentifizierungsmodus hinterlegt. Die nutzbaren Authentifizierungsmodi werden in der One Identity Manager-Datenbank gepflegt.


Weitere Informationen finden Sie unter [Authentifizierungsmodi](#) auf Seite 51.

- **Präfixe**  
Präfixe sind die relativen URLs einer Webanwendung, unterhalb der Websitesammlungen angelegt werden können.  
Weitere Informationen finden Sie unter [Präfixe](#) auf Seite 52.
- **Zonen und alternative URLs**  
In der One Identity Manager-Datenbank sind alle Zonen hinterlegt, die für eine Webanwendung konfiguriert werden können.  
Weitere Informationen finden Sie unter [Zonen und alternative URLs](#) auf Seite 52.
- **Webvorlagen**  
Webvorlagen werden genutzt, um Websites anzulegen.  
Weitere Informationen finden Sie unter [SharePoint Webvorlagen](#) auf Seite 53.
- **Berechtigungen**  
Über SharePoint Berechtigungen werden Benutzern Berechtigungen auf die Objekte einer SharePoint Website oder einer Webanwendung vergeben. Berechtigungen werden in Berechtigungsstufen und Berechtigungsrichtlinien zusammengefasst.  
Weitere Informationen finden Sie unter [SharePoint Berechtigungen](#) auf Seite 53.
- **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 [Nachbehandlung ausstehender Objekte](#) auf Seite 37.
- **Server**  
Für die Verarbeitung der zielsystemspezifischen Prozesse im One Identity Manager muss der Synchronisationsserver mit seinen Serverfunktionen bekannt sein.  
Weitere Informationen finden Sie unter [Bearbeiten eines Servers](#) auf Seite 54.
- **Zielsystemverantwortliche**  
Im One Identity Manager ist eine Standardanwendungsrolle für die Zielsystemverantwortlichen vorhanden. Weisen Sie dieser Anwendungsrolle die Identitäten zu, die berechtigt sind, alle SharePoint Farmen im One Identity Manager zu bearbeiten.  
Wenn Sie die Berechtigungen der Zielsystemverantwortlichen auf einzelne SharePoint Farmen einschränken wollen, definieren Sie weitere Anwendungsrollen. Die Anwendungsrollen müssen der Standardanwendungsrolle untergeordnet sein.  
Weitere Informationen finden Sie unter [Zielsystemverantwortliche](#) auf Seite 60.

# Authentifizierungsmodi

Für die Anmeldung am SharePoint Server unterstützt der One Identity Manager sowohl die forderungsbasierte Authentifizierung als auch die klassische Windows-Authentifizierung. An den Webanwendungen und an den Benutzerkonten ist der verwendete Authentifizierungsmodus hinterlegt. Die nutzbaren Authentifizierungsmodi werden in der One Identity Manager-Datenbank gepflegt. Der One Identity Manager liefert standardmäßig die Authentifizierungsmodi „Windows (Claims)“ (= forderungsbasierte Windows-Authentifizierung) und „Windows Classic Mode“ (= klassische Windows-Authentifizierung) mit. Wenn in Ihrer SharePoint-Umgebung andere Authentifizierungsmodi zur Anmeldung genutzt werden, legen Sie dafür separate Authentifizierungsmodi im One Identity Manager an. Damit ist eine Zuordnung der Benutzerkonten zu den Authentifizierungsmodi möglich. Erfassen Sie die Informationen zum Benutzerpräfix und Gruppenpräfix. Diese werden benötigt, um neue SharePoint Benutzerkonten im One Identity Manager anzulegen.

## Um einen Authentifizierungsmodus anzulegen

1. Wählen Sie die Kategorie **SharePoint | Basisdaten zur Konfiguration | Authentifizierungsmodi**.
2. Klicken Sie in der Ergebnisliste .
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Für einen eigenen Authentifizierungsmodus erfassen Sie folgende Stammdaten.

**Tabelle 7: Eigenschaften eines Authentifizierungsmodus**

Eigenschaft	Beschreibung
System ID	Beliebige Bezeichnung des Authentifizierungsmodus.
Benutzerpräfix	Präfix zur Bildung eines Anmeldenamens für neue Benutzerkonten. Das zugehörige Authentifizierungsobjekt ist keine Gruppe. Das heißt, am Benutzerkonto ist die Option <b>Gruppe</b> deaktiviert.
Gruppenpräfix	Präfix zur Bildung eines Anmeldenamens für neue Benutzerkonten. Das zugehörige Authentifizierungsobjekt ist eine Gruppe. Das heißt, am Benutzerkonto ist die Option <b>Gruppe</b> aktiviert.
Spalte für Anmeldeame	Spalte aus der Tabelle Person, die zur Bildung des Anmeldenamens für neue Benutzerkonten genutzt wird. Diese Information wird benötigt, wenn Identitäten über die automatische Identitätenzuordnung mit den Benutzerkonten verbunden werden sollen.

### ***Um einen eigenen Authentifizierungsmodus den Benutzerkonten automatisch zuzuordnen***

- Passen Sie im Designer die Bildungsregel für die Spalte SPSUser.UID\_SPSAuthSystem an.

Weitere Informationen finden Sie im One Identity Manager Konfigurationshandbuch.

## **Präfixe**

Präfixe sind die relativen URLs einer Webanwendung, unterhalb der Websitesammlungen angelegt werden können. Auf dem Überblicksformular werden die Eigenschaften der Präfixe, wie relativer Pfad, absoluter Pfad und Präfixtyp, sowie die zugehörige Webanwendung angezeigt.

### ***Um einen Überblick über ein Präfix zu erhalten***

1. Wählen Sie die Kategorie **SharePoint | Basisdaten zur Konfiguration | Präfixe**.
2. Wählen Sie in der Ergebnisliste das Präfix.
3. Wählen Sie die Aufgabe **Überblick über das SharePoint Präfix**.

## **Zonen und alternative URLs**

In der One Identity Manager-Datenbank sind alle Zonen hinterlegt, die für eine Webanwendung konfiguriert werden können. Auf dem Überblicksformular für eine Zone werden die alternativen URLs angezeigt, die für den Zugriff auf die Webanwendungen konfiguriert sind.

### ***Um einen Überblick über eine Zone zu erhalten***

1. Wählen Sie die Kategorie **SharePoint | Basisdaten zur Konfiguration | Zonen**.
2. Wählen Sie in der Ergebnisliste die Zone.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Zone**.

### ***Um einen Überblick über die alternativen URLs einer Webanwendung zu erhalten***

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | URLs**.
2. Wählen Sie in der Ergebnisliste eine URL.
3. Wählen Sie die Aufgabe **Überblick über die alternative URL**.

# SharePoint Webvorlagen

Webvorlagen werden genutzt, um Websites anzulegen. Wenn neue Websites mit dem One Identity Manager angelegt werden sollen, lesen Sie die Webvorlagen durch die Synchronisation in die One Identity Manager-Datenbank ein. Auf dem Überblicksformular werden die Sprachen angezeigt, in der eine Webvorlage zur Verfügung steht.

## *Um einen Überblick über eine Webvorlage zu erhalten*

1. Wählen Sie die Kategorie **SharePoint | Basisdaten zur Konfiguration | Webvorlagen**.
2. Wählen Sie in der Ergebnisliste die Webvorlage.
3. Wählen Sie die Aufgabe **Überblick über die Webvorlage**.

# SharePoint Berechtigungen

Über SharePoint Berechtigungen werden Benutzern Berechtigungen auf die Objekte einer SharePoint Website oder einer Webanwendung vergeben. Berechtigungen werden in Berechtigungsstufen und Berechtigungsrichtlinien zusammengefasst. Auf dem Überblicksformular einer Berechtigung werden alle Berechtigungsrichtlinien der Webanwendungen angezeigt, denen die Berechtigung explizit erteilt oder verweigert wurde.

In einer SharePoint-Umgebung kann die Menge der Berechtigungen, die an Berechtigungsstufen zugewiesen werden kann, eingeschränkt werden. Sie erhalten einen Überblick, für welche Webanwendungen eine Berechtigung zugelassen ist.

## *Um einen Überblick über eine Berechtigung zu erhalten*

1. Wählen Sie die Kategorie **SharePoint | Basisdaten zur Konfiguration | Berechtigungen**.
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Berechtigung**.

Berechtigungen können im One Identity Manager an Berechtigungsstufen zugewiesen werden.

## *Um eine zulässige Berechtigung an Berechtigungsstufen zuzuweisen*

1. Wählen Sie die Kategorie **SharePoint | Basisdaten zur Konfiguration | Berechtigungen**.
2. Wählen Sie in der Ergebnisliste die Berechtigung.
3. Wählen Sie die Aufgabe **Berechtigungsstufen zuweisen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungsstufen zu.  
- ODER -  
Entfernen Sie im Bereich **Zuordnungen entfernen** die Berechtigungsstufen.
5. Speichern Sie die Änderungen.

### Verwandte Themen

- [SharePoint Rollen und Berechtigungsstufen](#) auf Seite 144

## SharePoint Kontingente

Auf dem Überblicksformular für ein Kontingent werden die SharePoint Farm abgebildet und die Websitesammlungen, denen das Kontingent zugewiesen ist.

### *Um einen Überblick über ein Kontingent zu erhalten*

1. Wählen Sie die Kategorie **SharePoint | Kontingente**.
2. Wählen Sie in der Ergebnisliste das Kontingent.
3. Wählen Sie die Aufgabe **Überblick über das SharePoint Kontingent**.

## SharePoint Sprachen

In der One Identity Manager-Datenbank werden alle Sprachen abgebildet, für die in der SharePoint-Umgebung Sprachpakete installiert sind.

### *Um einen Überblick über eine Sprache zu erhalten*

1. Wählen Sie die Kategorie **SharePoint | Baumdarstellung | <Farm> | Sprachen**.
2. Wählen Sie in der Ergebnisliste die Sprache.
3. Wählen Sie die Aufgabe **Überblick über die Sprache**.

## Bearbeiten eines Servers

Für die Verarbeitung der zielsystemspezifischen Prozesse im One Identity Manager muss der Synchronisationsserver mit seinen Serverfunktionen bekannt sein. Um die Funktion eines Servers zu definieren, haben Sie mehrere Möglichkeiten:

- Erstellen Sie im Designer in der Kategorie **Basisdaten > Installationen > Jobserver** einen Eintrag für den Jobserver. Ausführliche Informationen dazu finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Wählen Sie im Manager in der Kategorie **SharePoint | Basisdaten zur Konfiguration | Server** einen Eintrag für den Jobserver aus und bearbeiten Sie die Stammdaten des Jobservers.

Nutzen Sie dieses Verfahren, wenn der Jobserver bereits im One Identity Manager bekannt ist und Sie für den Jobserver spezielle Funktionen konfigurieren möchten.

**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 **SharePoint > Basisdaten zur Konfiguration > Server**.
2. Wählen Sie in der Ergebnisliste den Jobserver-Eintrag.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für den Jobserver.
5. Wählen Sie die Aufgabe **Serverfunktionen zuweisen** und legen Sie die Serverfunktionen fest.
6. Speichern Sie die Änderungen.

### **Detaillierte Informationen zum Thema**

- [Stammdaten eines Jobservers](#) auf Seite 55
- [Festlegen der Serverfunktionen](#) auf Seite 58

### **Verwandte Themen**

- [Einrichten des Synchronisationsservers](#) auf Seite 16

## **Stammdaten eines Jobservers**

**HINWEIS:** Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten > Installationen > Jobserver** zur Verfügung.

**HINWEIS:** Abhängig von den installierten Modulen können weitere Eigenschaften verfügbar sein.

**Tabelle 8: Eigenschaften eines Jobservers**

<b>Eigenschaft</b>	<b>Bedeutung</b>
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS-Syntax. Syntax: <Name des Servers>.<Vollqualifizierter Domänenname>
Zielsystem	Zielsystem des Computerkontos.
Sprache	Sprache des Servers.
Server ist Cluster	Gibt an, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. <b>HINWEIS:</b> Die Eigenschaften <b>Server ist Cluster</b> und <b>Server gehört zu Cluster</b> 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.
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 <b>Win32</b> , <b>Windows</b> ,



Eigenschaft	Bedeutung
	<b>Linux</b> und <b>Unix</b> . Ist die Angabe leer, wird <b>Win32</b> angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen.
One Identity Manager Service installiert	<p>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.</p> <p>Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.</p>
Stopp One Identity Manager Service	<p>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.</p> <p>Den Dienst können Sie mit entsprechenden administrativen Berechtigungen im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im <i>One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche</i>.</p>
Pausiert wegen Nichtverfügbarkeit eines Zielsystems	<p>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.</p> <p>Ausführliche Informationen zum Offline-Modus finden Sie im <i>One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation</i>.</p>
Kein automatisches Softwareupdate	<p>Gibt an, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist.</p> <p><b>HINWEIS:</b> Server, für welche die Option aktiviert ist,</p>

Eigenschaft	Bedeutung
	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 58

# 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 9: Zulässige Serverfunktionen**

Serverfunktion	Anmerkungen
Active Directory Konnektor	Server, auf dem der Active Directory Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem Active Directory aus.
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.

Serverfunktion	Anmerkungen
Aktualisierungsserver	<p>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.</p> <p>Bei der initialen Schemainstallation wird der Server, auf dem die One Identity Manager-Datenbank installiert ist, mit dieser Serverfunktion gekennzeichnet.</p>
SQL Ausführungsserver	<p>Der Server kann SQL Aufträge ausführen. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist.</p> <p>Für eine Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.</p>
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.
SharePoint Konnektor	Server, auf dem der SharePoint Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem SharePoint aus.
SMTP Host	Server, auf dem durch den One Identity Manager Service E-Mail Benachrichtigungen verschickt werden. Voraussetzung zum Versenden von Mails durch den One Identity Manager Service ist ein konfigurierter

Serverfunktion	Anmerkungen
	SMTP Host.
Standard Berichtsserver	Server, auf dem die Berichte generiert werden.
Windows PowerShell Konnektor	Der Server kann Windows PowerShell Version 3.0 oder neuer ausführen.

## Verwandte Themen

- [Stammdaten eines Jobservers](#) auf Seite 55

# Zielsystemverantwortliche

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

Wenn Sie die Berechtigungen der Zielsystemverantwortlichen auf einzelne SharePoint Farmen 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 Identitäten als Zielsystemadministratoren fest.
2. Die Zielsystemadministratoren nehmen die Identitäten in die Standardanwendungsrolle für die Zielsystemverantwortlichen auf.  
Zielsystemverantwortliche der Standardanwendungsrolle sind berechtigt alle SharePoint Farmen im One Identity Manager zu bearbeiten.
3. Zielsystemverantwortliche können innerhalb ihres Verantwortungsbereiches weitere Identitäten als Zielsystemverantwortliche berechtigen und bei Bedarf weitere untergeordnete Anwendungsrollen erstellen und einzelnen SharePoint Farmen zuweisen.

**Tabelle 10: Standardanwendungsrolle für Zielsystemverantwortliche**

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle <b>Zielsysteme   SharePoint</b> oder einer untergeordneten Anwendungsrolle zugewiesen sein.

Benutzer	Aufgaben
	<p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> <li>• Übernehmen die administrativen Aufgaben für das Zielsystem.</li> <li>• Erzeugen, ändern oder löschen die Zielsystemobjekte.</li> <li>• Bearbeiten Kennwortrichtlinien für das Zielsystem.</li> <li>• Bereiten Systemberechtigungen zur Aufnahme in den IT Shop vor.</li> <li>• Können Identitäten anlegen, die nicht den Identitätstyp <b>Primäre Identität</b> haben.</li> <li>• Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.</li> <li>• Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation.</li> <li>• Berechtigen innerhalb ihres Verantwortungsbereiches weitere Identitäten als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.</li> </ul>

#### ***Um initial Identitäten 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 **Identitäten zuweisen**.
4. Weisen Sie die Identität zu und speichern Sie die Änderung.

#### ***Um initial Identitäten 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 > SharePoint**.
3. Wählen Sie die Aufgabe **Identitäten zuweisen**.
4. Weisen Sie die Identitäten zu und speichern Sie die Änderungen.

### **Um als Zielsystemverantwortlicher weitere Identitäten als Zielsystemverantwortliche zu berechtigen**

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie in der Kategorie **SharePoint > Basisdaten zur Konfiguration > Zielsystemverantwortliche** die Anwendungsrolle.
3. Wählen Sie die Aufgabe **Identitäten zuweisen**.
4. Weisen Sie die Identitäten zu und speichern Sie die Änderungen.

### **Um Zielsystemverantwortliche für einzelne SharePoint Farmen festzulegen**

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **SharePoint > Farmen**.
3. Wählen Sie in der Ergebnisliste die Farm.
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 | SharePoint** zu.
  - b. Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.
6. Speichern Sie die Änderungen.
7. Weisen Sie der Anwendungsrolle die Identitäten zu, die berechtigt sind, die Farm im One Identity Manager zu bearbeiten.

### **Verwandte Themen**

- [One Identity Manager Benutzer für die Verwaltung einer SharePoint-Umgebung](#) auf Seite 10
- [Allgemeine Stammdaten einer SharePoint Farm](#) auf Seite 83

## **Einrichten von Kontendefinitionen**

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

Aus den Identitätenstammdaten resultieren die Daten für das Benutzerkonto im jeweiligen Zielsystem. Über die primäre Zuordnung der Identität 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 Identität geregelt. Die Verarbeitung erfolgt über Bildungsregeln. In der Standardinstallation sind vordefinierte Bildungsregeln zur Ermittlung der benötigten Daten für die Benutzerkonten enthalten. Bei Bedarf können Sie die Bildungsregeln kundenspezifisch anpassen.

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


**HINWEIS:** Über Kontendefinitionen können nur SharePoint Benutzerkonten erstellt werden, die nicht als Gruppe gekennzeichnet sind (`IsDomainGroup = 'False'`). Es wird jedoch empfohlen SharePoint Benutzerkonten auf der Basis von Zielsystemgruppen zu erstellen. Nutzen Sie Kontendefinitionen für SharePoint nur, wenn Sie nicht dem empfohlenen Vorgehen folgen. Weitere Informationen finden Sie unter [SharePoint Benutzerkonten](#) auf Seite 96.

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

- [Erstellen einer Kontendefinition](#)
- [Erstellen der Automatisierungsgrade](#)
- [Erstellen einer Abbildungsvorschrift für IT Betriebsdaten](#)
- [Erfassen der IT Betriebsdaten](#)
- [Zuweisen der Kontendefinition an Identitäten](#)
- [Zuweisen der Kontendefinition an ein Zielsystem](#)

## Erstellen einer Kontendefinition

### *Um eine Kontendefinition zu bearbeiten oder zu erstellen*

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

# Stammdaten einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

**Tabelle 11: Stammdaten einer Kontendefinition**

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte Kontendefinition	<p>Angabe der vorausgesetzten Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch zugeordnet.</p> <p><b>TIPP:</b> Sie können hier die Kontendefinition der zugehörigen Active Directory oder LDAP Domäne eintragen. In diesem Fall wird für die Identität zunächst ein Active Directory bzw. LDAP Benutzerkonto erzeugt. Ist dieses vorhanden, wird das SharePoint Benutzerkonto angelegt.</p> <p>Dieses Verhalten ist unternehmensspezifisch zu implementieren. Passen Sie den Prozess TSB_PersonHasAccountDef_AutoCreate_SPSUser dafür unternehmensspezifisch an.</p>
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatisierungsgrad (initial)	Standardautomatisierungsgrad, der bei Neuanlage von Benutzerkonten standardmäßig verwendet werden soll.
Risikoindex	<p>Wert zur Bewertung des Risikos von Zuweisungen der Kontendefinition an Identitäten. Stellen Sie einen Wert im Bereich von <b>0</b> bis <b>1</b> ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter <b>QER   CalculateRiskIndex</b> aktiviert ist.</p> <p>Ausführliche Informationen finden Sie im <i>One Identity Manager Administrationshandbuch für Risikobewertungen</i>.</p>
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 bestellt



Eigenschaft	Beschreibung
	werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Identitäten 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 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 Identitäten	<p>Gibt an, ob die Kontendefinition automatisch an alle internen Identitäten zugewiesen werden soll. Um die Kontendefinition automatisch an alle internen Identitäten zuzuweisen, verwenden Sie die Aufgabe <b>Automatische Zuweisung zu Identitäten aktivieren</b>. Die Kontendefinition wird an jede Identität zugewiesen, die nicht als extern markiert ist. Sobald eine neue interne Identität erstellt wird, erhält diese Identität ebenfalls automatisch diese Kontendefinition.</p> <p>Um die automatische Zuweisung der Kontendefinition von allen Identitäten zu entfernen, verwenden Sie die Aufgabe <b>Automatische Zuweisung zu Identitäten deaktivieren</b>. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Identitäten zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.</p>
Kontendefinition bei dauerhafter Deaktivierung beibehalten	<p>Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Identitäten.</p> <p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>
Kontendefinition bei zeitweiliger Deaktivierung beibehalten	<p>Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Identitäten.</p> <p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>
Kontendefinition bei verzögertem Löschen beibehalten	Angabe zur Zuweisung der Kontendefinition bei verzögertem Löschen von Identitäten.

Eigenschaft	Beschreibung
	<p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>
Kontendefinition bei Sicherheitsgefährdung beibehalten	<p>Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Identitäten.</p> <p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>
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	<p>Gibt an, ob das Benutzerkonto Gruppen über die verbundene Identität erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt.</p> <ul style="list-style-type: none"> <li>• Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen.</li> <li>• Wenn eine Identität eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Identität diese Gruppe nur, wenn die Option aktiviert ist.</li> </ul>
Rollen erbbar	Gibt an, ob das Benutzerkonto SharePoint Rollen über die verbundene Identität erben darf. Ist die Option aktiviert, werden die Rollen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt.

# Erstellen der Automatisierungsgrade

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

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

One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

- **Unmanaged**: Benutzerkonten mit dem Automatisierungsgrad **Unmanaged** erhalten eine Verbindung zur Identität, erben jedoch keine weiteren Eigenschaften. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Identität werden initial einige der Identitätseigenschaften übernommen. Werden die Identitätseigenschaften 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 Identität. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Identität werden initial die Identitätseigenschaften übernommen. Werden die Identitätseigenschaften 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 Identität 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 Identität deaktiviert, gelöscht oder als sicherheitsgefährdend eingestuft wird, können die Benutzerkonten der Identität gesperrt werden. Wird die Identität 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 Identität gesperrt sind und somit auch nicht in Gruppen Mitglied sein dürfen. Während dieser Zeit sollen keine Vererbungsvorgänge für diese

Identitäten berechnet werden. Bestehende Gruppenmitgliedschaften werden dann gelöscht!

**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 **SharePoint > 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.

### **Um einen Automatisierungsgrad zu bearbeiten**

1. Wählen Sie im Manager die Kategorie **SharePoint > Basisdaten zur Konfiguration > Kontendefinitionen > Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.  
-ODER-  
Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Automatisierungsgrades.
4. Speichern Sie die Änderungen.

## **Stammdaten eines Automatisierungsgrades**

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

**Tabelle 12: Stammdaten eines Automatisierungsgrades**

<b>Eigenschaft</b>	<b>Beschreibung</b>
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:

Eigenschaft	Beschreibung
	<ul style="list-style-type: none"> <li>• <b>Niemals:</b> Die Daten werden nicht aktualisiert. (Standard)</li> <li>• <b>Immer:</b> Die Daten werden immer aktualisiert.</li> <li>• <b>Nur initial:</b> Die Daten werden nur initial ermittelt.</li> </ul>
Gruppen bei zeitweiliger Deaktivierung beibehalten	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Identitäten ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei zeitweiliger Deaktivierung sperren *)	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Identitäten gesperrt werden sollen.
Gruppen bei dauerhafter Deaktivierung beibehalten	Gibt an, ob die Benutzerkonten dauerhaft deaktivierter Identitäten ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei dauerhafter Deaktivierung sperren *)	Gibt an, ob die Benutzerkonten dauerhaft deaktivierter Identitäten gesperrt werden sollen.
Gruppen bei verzögertem Löschen beibehalten	Gibt an, ob die Benutzerkonten zum Löschen markierter Identitäten ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei verzögertem Löschen sperren *)	Gibt an, ob die Benutzerkonten zum Löschen markierter Identitäten gesperrt werden sollen.
Gruppen bei Sicherheitsgefährdung beibehalten	Gibt an, ob die Benutzerkonten von sicherheitsgefährdenden Identitäten ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei Sicherheitsgefährdung sperren *)	Gibt an, ob die Benutzerkonten von sicherheitsgefährdenden Identitäten gesperrt werden sollen.
Gruppen bei deaktiviertem Benutzerkonto beibehalten	Gibt an, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen.

**HINWEIS:** \*) SharePoint Benutzerkonten können nicht gesperrt werden!

Wenn eine Identität deaktiviert, verzögert gelöscht oder als sicherheitsgefährdend eingestuft wird, bleiben deren SharePoint Benutzerkonten aktiv. Für die Anmeldung an einer SharePoint Websitesammlung ist relevant, ob das als Authentifizierungsobjekt verbundene Benutzerkonto gesperrt oder deaktiviert ist. Um zu verhindern, dass sich eine Identität, die deaktiviert, gelöscht oder als sicherheitsgefährdend eingestuft ist, an einer SharePoint Websitesammlung anmeldet, verwalten Sie die als Authentifizierungsobjekte verbundenen Benutzerkonten über Kontendefinitionen.

# Erstellen einer Abbildungsvorschrift für IT Betriebsdaten

Eine Kontendefinition legt fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über die primären Rollen einer Identität 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 Identität im Zielsystem verwendet.

- SharePoint Authentifizierungsmodus
- SharePoint Online Authentifizierungsmodus
- Gruppen erbbar
- Rollen erbbar
- Identität
- Privilegiertes Benutzerkonto

## Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

1. Wählen Sie im Manager die Kategorie **SharePoint > 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 Identität, 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 **Identität - Erstellung neues Benutzerkontos mit Standardwerten** verwendet.

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

5. Speichern Sie die Änderungen.

## Erfassen der IT Betriebsdaten

Um für eine Identität 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 Identität 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 Abbildungsvorschrift der IT Betriebsdaten für die Kontendefinitionen A und B legen Sie die Eigenschaft **Abteilung** zur Ermittlung der gültigen IT Betriebsdaten 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.

## 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 Identität 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 **SharePoint > 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 Kontendefinition an Identitäten**

Kontendefinitionen werden an die Identitäten des Unternehmens zugewiesen.

Das Standardverfahren für die Zuweisung von Kontendefinitionen an Identitäten ist die indirekte Zuweisung. Die Kontendefinitionen werden an die Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen zugewiesen. Die Identitäten 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 Identitäten zugewiesen werden.

Kontendefinitionen können automatisch an alle Identitäten 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 Identitäten zugewiesen werden oder als Produkte in den IT Shop aufgenommen werden.

In den Prozessen der One Identity Manager Standardinstallation wird zunächst überprüft, ob die Identität 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 Identität wirksam ist, behält die Identität ihr daraus entstandenes Benutzerkonto. Wird die Zuweisung einer Kontendefinition entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht. Benutzerkonten, die als **Ausstehend** markiert sind, werden nur gelöscht, wenn der Konfigurationsparameter **QER | Person | User | DeleteOptions | DeleteOutstanding** aktiviert ist.

## Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Identitäten

- Für die Rollenklasse (Abteilung, Kostenstelle, Standort oder Geschäftsrolle) ist die Zuweisung von Identitäten 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*.

# Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen


Weisen Sie die Kontendefinition an Abteilungen, Kostenstellen oder Standorte zu, damit die Kontendefinitionen über diese Organisationen an Identitäten zugewiesen werden.

## *Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen*

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

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

### *Um eine Zuweisung zu entfernen*

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

# Kontendefinition an Geschäftsrollen zuweisen

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


Weisen Sie die Kontendefinition an Geschäftsrollen zu, damit die Kontendefinitionen über diese Geschäftsrollen an Identitäten zugewiesen werden.

## *Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen*

1. Wählen Sie im Manager die Kategorie **SharePoint > 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.

## Kontendefinition an alle Identitäten zuweisen

Über diese Aufgaben wird die Kontendefinition an alle internen Identitäten zugewiesen. Identitäten, die als externe Identitäten gekennzeichnet sind, erhalten die Kontendefinition nicht. Sobald eine neue interne Identität erstellt wird, erhält diese Identität 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 Identitäten sowie alle zukünftig neu hinzuzufügenden internen Identitäten ein Benutzerkonto in diesem Zielsystem erhalten sollen!

### Um eine Kontendefinition an alle Identitäten zuzuweisen

1. Wählen Sie im Manager die Kategorie **SharePoint > 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 Identitäten aktivieren**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Speichern Sie die Änderungen.

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

## Kontendefinition direkt an Identitäten zuweisen

Kontendefinitionen können direkt oder indirekt an Identitäten zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung des Identitäten und der Kontendefinitionen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen.


Um auf Sonderanforderungen schnell zu reagieren, können Sie die Kontendefinitionen auch direkt an die Identitäten zuweisen.

### **Um eine Kontendefinition direkt an Identitäten zuzuweisen**

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

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

#### **Um eine Zuweisung zu entfernen**

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

## **Kontendefinition an Systemrollen zuweisen**

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

Mit dieser Aufgabe nehmen Sie eine Kontendefinition in Systemrollen auf.


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

### **Um Kontendefinitionen in eine Systemrolle aufzunehmen**

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

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

#### **Um eine Zuweisung zu entfernen**

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

## **Kontendefinition in den IT Shop aufnehmen**

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

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

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

- Soll die Kontendefinition nur über IT Shop-Bestellungen an Identitäten 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 **SharePoint > 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 **SharePoint > 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 **SharePoint > 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 einer Kontendefinition](#) auf Seite 64
- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 75
- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 75

- [Kontendefinition direkt an Identitäten zuweisen](#) auf Seite 76
- [Kontendefinition an Systemrollen zuweisen](#) auf Seite 77

## Zuweisen der Kontendefinition an ein Zielsystem

Wenn Sie die automatische Zuordnung von Benutzerkonten und Identitäten 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 Identität 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 **SharePoint > Websitesammlungen** die Websitesammmlung.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie in der Auswahlliste **Kontendefinition (initial)** die Kontendefinition für die Benutzerkonten.
4. Speichern Sie die Änderungen.

## Löschen einer Kontendefinition

Sie können Kontendefinitionen löschen, wenn diese keinem Zielsystem, keiner Identität, 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 Identitäten.
  - a. Wählen Sie im Manager die Kategorie **SharePoint > 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 Identitäten deaktivieren**.



- e. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
  - f. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Identitäten.
    - a. Wählen Sie im Manager die Kategorie **SharePoint > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
    - b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    - c. Wählen Sie die Aufgabe **An Identitäten zuweisen**.
    - d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Identitäten.
    - e. Speichern Sie die Änderungen.
  3. Entfernen Sie die Zuordnung der Kontendefinition zu Abteilungen, Kostenstellen und Standorten.
    - a. Wählen Sie im Manager die Kategorie **SharePoint > 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 **SharePoint > 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 **SharePoint > 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 **SharePoint > 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 **SharePoint > Websitesammlungen** die Websitesammmlung.
  - 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 **SharePoint > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
  - b. Wählen Sie in der Ergebnisliste die Kontendefinition.
  - c. Klicken Sie , um die Kontendefinition zu löschen.

## SharePoint Farmen

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

### Um die Stammdaten einer Farm zu bearbeiten


1. Wählen Sie die Kategorie **SharePoint | Farmen**.
2. Wählen Sie in der Ergebnisliste die Farm. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Bearbeiten Sie die Stammdaten der Farm.
4. Speichern Sie die Änderungen.

## Allgemeine Stammdaten einer SharePoint Farm

Für eine Farm erfassen Sie folgende allgemeine Stammdaten.

**Tabelle 13: Allgemeine Stammdaten einer Farm**

Eigenschaft	Beschreibung
Bezeichnung	Name der SharePoint-Instanz. Daraus wird ein definierter Name zur internen Nutzung gebildet.
Domäne	Name der Active Directory oder LDAP Domäne, die als Security Provider für die SharePoint Umgebung dient. Die referenzierten Benutzerkonten und Gruppen werden in dieser Domäne gesucht.
Anzeigename	Anzeigename für die Farm.
Zielsystemverantwortliche	Anwendungsrolle, in der die Zielsystemverantwortlichen der Farm festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte der Farm, der sie zugeordnet sind. Jeder

Eigenschaft	Beschreibung									
	<p>Farm können andere Zielsystemverantwortliche zugeordnet werden.</p> <p>Wählen Sie die One Identity Manager Anwendungsrolle aus, deren Mitglieder verantwortlich für die Administration dieser Farm sind. Über die Schaltfläche  neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.</p>									
Synchronisiert durch	<p>Art der Synchronisation, über welche die Daten zwischen der Farm und dem One Identity Manager ausgetauscht werden. Sobald Objekte für diese Farm im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden.</p> <p>Beim Erstellen einer Farm mit dem Synchronization Editor wird <b>One Identity Manager</b> verwendet.</p> <p><b>Tabelle 14: Zulässige Werte</b></p> <table><tr><th>Wert</th><th>Synchro- nisation durch</th><th>Provi- sionierung durch</th></tr><tr><td>One Identity Manage- r</td><td>SharePoint Konnektor</td><td>SharePoint Konnektor</td></tr><tr><td>Keine Synchro- nisation</td><td>keine</td><td>keine</td></tr></table> <p><b>HINWEIS:</b> Wenn Sie <b>Keine Synchronisation</b> festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.</p>	Wert	Synchro- nisation durch	Provi- sionierung durch	One Identity Manage- r	SharePoint Konnektor	SharePoint Konnektor	Keine Synchro- nisation	keine	keine
Wert	Synchro- nisation durch	Provi- sionierung durch								
One Identity Manage- r	SharePoint Konnektor	SharePoint Konnektor								
Keine Synchro- nisation	keine	keine								
Build-Version	Die Build-Version der SharePoint Services dieser Farm wird durch die Synchronisation eingelesen.									

## Verwandte Themen

- [Zielsystemverantwortliche](#) auf Seite 60

# Synchronisationsprojekt bearbeiten

Synchronisationsprojekte, in denen eine Farm bereits als Basisobjekt verwendet wird, können auch über den Manager geöffnet werden. In diesem Modus können beispielsweise die Konfigurationseinstellungen überprüft oder die Synchronisationsprotokolle eingesehen werden. Der Synchronization Editor wird nicht mit seinem vollen Funktionsumfang

gestartet. Verschiedene Funktionen, wie Simulieren oder Ausführen einer Synchronisation, Starten des Zielsystembrowsers und andere, können nicht ausgeführt werden.

**HINWEIS:** Der Manager ist währenddessen für die Bearbeitung gesperrt. Um Objekte im Manager bearbeiten zu können, schließen Sie den Synchronization Editor.

### **Um ein bestehendes Synchronisationsprojekt im Synchronization Editor zu öffnen**

1. Wählen Sie die Kategorie **SharePoint | Farmen**.
2. Wählen Sie in der Ergebnisliste die Farm. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten....**

### **Detaillierte Informationen zum Thema**

- One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation

### **Verwandte Themen**

- [Anpassen einer Synchronisationskonfiguration](#) auf Seite 30

## SharePoint Webanwendungen

SharePoint Webanwendungen halten Berechtigungen für SharePoint Benutzer vor, die übergreifend für alle Websites innerhalb der Webanwendung gelten. Über das Überblicksformular erhalten Sie Informationen über die Objekte der SharePoint-Umgebung, in welche die Webanwendung eingebunden ist. Es werden die für die Webanwendung definierten Benutzer- und Berechtigungsrichtlinien angezeigt. An Webanwendungen, für welche die forderungsbasierte Authentifizierung zugelassen ist, werden die zulässigen SharePoint Provider angezeigt.

Im SharePoint kann die Menge der Berechtigungen, die an SharePoint Berechtigungsstufen zugewiesen werden kann, eingeschränkt werden. Auf dem Überblicksformular sehen Sie alle für die Webanwendung zulässigen Berechtigungen.

### ***Um einen Überblick über eine Webanwendung zu erhalten***

1. Wählen Sie die Kategorie **SharePoint | Webanwendungen**.
2. Wählen Sie in der Ergebnisliste die Webanwendung.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Webanwendung**.

### **Verwandte Themen**

- [SharePoint Rollen und Berechtigungsstufen](#) auf Seite 144

# SharePoint Websitesammlungen und Websites

SharePoint Websites werden in Websitesammlungen organisiert. Eine Websitesammlung verwaltet Zugriffsrechte und Gestaltungsvorlagen für alle Websites der Websitesammlung. Sie besteht mindestens aus einer Website auf oberster Ebene - der Root-Site. Weitere Websites sind dieser Root-Site untergeordnet. Sie können durch einfache Vorgängerbeziehungen zu Hierarchien verbunden werden. Durch diese hierarchische Struktur können Eigenschaften (beispielsweise Rollendefinitionen) an untergeordnete Websites vererbt werden.

Im One Identity Manager werden Websitesammlungen und Websites mit ihren Zugriffsrechten abgebildet. Ihre Eigenschaften können im One Identity Manager nicht bearbeitet werden. Die innerhalb einer Websitesammlung verwalteten Zugriffsrechte können im One Identity Manager bearbeitet werden. Dafür werden SharePoint Rollen, Gruppen und Benutzerkonten in die One Identity Manager-Datenbank eingelesen.

## Verwandte Themen

- [SharePoint Rollen und Gruppen](#) auf Seite 123
- [SharePoint Benutzerkonten](#) auf Seite 96

## SharePoint Websitesammlungen

Eine Websitesammlung fasst die einander untergeordneten Websites zusammen. Hier werden Benutzerkonten und deren Zugriffsberechtigungen auf die Websites verwaltet. Um die automatische Zuordnung von Benutzerkonten und Identitäten zu nutzen, weisen Sie der Websitesammlung eine Kontendefinition zu.

Auf dem Überblicksformular einer Websitesammlung werden die berechtigten Benutzerkonten und Gruppen dargestellt sowie die Webanwendung und die Root-Site, mit denen die Websitesammlung verbunden ist. Die einer Websitesammlung zugewiesene Kontingentvorlage, die Administratoren und Auditoren der Websitesammlung werden ebenfalls auf dem Überblicksformular abgebildet.

### Um die Eigenschaften einer Websitesammlung zu bearbeiten

1. Wählen Sie die Kategorie **SharePoint | Websitesammlungen**.
2. Wählen Sie in der Ergebnisliste die Websitesammlung aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

### Detaillierte Informationen zum Thema

- [Allgemeine Stammdaten einer Websitesammlung](#) auf Seite 88
- [Festlegen der Kategorien für die Vererbung von SharePoint Gruppen](#) auf Seite 89

## Allgemeine Stammdaten einer Websitesammlung

Für Websitesammlungen werden die folgende Stammdaten abgebildet.

**Tabelle 15: Allgemeine Stammdaten einer Websitesammlung**

Eigenschaft	Beschreibung
Kontendefinition	Initiale Kontendefinition zur Erzeugung von Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für diese Websitesammlung die automatische Zuordnung von Identitäten zu Benutzerkonten genutzt wird und dabei bereits verwaltete Benutzerkonten (Zustand <b>Linked configured</b> ) entstehen sollen. Es wird der Standardautomatisierungsgrad der Kontendefinition angewendet.  Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Identität verbunden (Zustand <b>Linked</b> ). Dies ist beispielsweise bei der initialen Synchronisation der Fall.
Server	Name des SharePoint Servers, der die Websitesammlung bereitstellt.
Webanwendung	Eindeutige Kennung der Webanwendung, zu der die Websitesammlung gehört.
Root-Site	Verweis auf die Root-Site dieser Websitesammlung. Es wird auf eine Website verwiesen, bei der die Option <b>Root-Site</b> aktiviert ist.
Administrator	Benutzerkonto des Administrators der Websitesammlung.
Zusätzlicher Adminis-	Benutzerkonto des zusätzlichen Administrators der Websi-



Eigenschaft	Beschreibung
trator	tesammlung.
Verwendeter Speicherplatz	Information über den Speicherplatz, den die Websitesammlung auf dem Server belegt.
Letzte sicherheitsrelevante Änderung	Zeitpunkt der letzten sicherheitsrelevanten Änderung, die an einem Objekt dieser Websitesammlung vorgenommen wurde.

Auf dem Tabreiter **Adressen** werden die URL und der Port der Websitesammlung angezeigt sowie die URL eines mit der Websitesammlung verbundenen Portals.


## Verwandte Themen

- [Einrichten von Kontendefinitionen](#) auf Seite 62

# Festlegen der Kategorien für die Vererbung von SharePoint Gruppen

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

## Um Kategorien zu definieren

1. Wählen Sie im Manager in der Kategorie **SharePoint > Websitesammlungen** die Websitesammmlung.
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 SharePoint Gruppen anhand von Kategorien](#) auf Seite 140
- One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul

# SharePoint Websites

Websites können hierarchisch strukturiert werden. Für jede Websitesammlung gibt es immer eine Website, die als „Root-Site“ gekennzeichnet ist. Weitere Websites dieser Websitesammlung sind der Root-Site untergeordnet.

### Um die Eigenschaften einer Website anzuzeigen

1. Wählen Sie die Kategorie **SharePoint | Websites**.
2. Wählen Sie in der Ergebnisliste die Website. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

## Detaillierte Informationen zum Thema

- [Allgemeine Stammdaten einer Website](#) auf Seite 90
- [Adressdaten einer Website](#) auf Seite 91
- [Designinformationen einer Website](#) auf Seite 92

# Allgemeine Stammdaten einer Website

Für Websites werden die folgenden allgemeine Stammdaten abgebildet.

**Tabelle 16: Allgemeine Stammdaten einer Website**

Eigenschaft	Beschreibung
Anzeigename	Anzeigename der Website.
Root-Site	Angabe, ob die Website die Root-Site der Websitesammlung ist.
Übergeordnete Website	Eindeutige Kennung der übergeordneten Website.
Websitesammlung	Eindeutige Kennung der Websitesammlung, zu der die Website gehört.
Eigene Rollendefinitionen	Angabe, ob Berechtigungsstufen und die damit verbundenen Berechtigungen für die Website definiert werden können (Tabellen <code>SPSRole</code> und <code>SPSRoleHasSPSPermission</code> ). Ist die Option deaktiviert, werden die Rollendefinitionen von der übergeordneten Website

Eigenschaft	Beschreibung
	geerbt.
Rollen verwenden von	Eindeutige Kennung der Website, deren Rollendefinitionen geerbt werden. Sind der Website eigene Rollen zugewiesen, werden deren Berechtigungen durch die geerbten Berechtigungen überschrieben.
Eigene Rollenzuweisungen	Angabe, ob Benutzerkonten oder Gruppen direkt auf die Website berechtigt werden können (Tabellen SPSUserHasSPSRLAsgn und SPSGroupHasSPSRLAsgn). Ist die Option deaktiviert, werden die Rollenzuweisungen von der übergeordneten Website geerbt. Es können keine weiteren Benutzerkonten oder Gruppen auf die Website berechtigt werden.
Zuweisungen verwenden von	Eindeutige Kennung der Website, deren Rollenzuweisungen geerbt werden.
Autor	Verweis auf das Benutzerkonto, mit dem die Website erstellt wurde.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Anonymer Zugriff erlaubt	Angabe, ob ein anonymer Zugriff auf die Website erlaubt ist.

## Detaillierte Informationen zum Thema

- [SharePoint Rollen und Gruppen](#) auf Seite 123
- [SharePoint Rollen und Berechtigungsstufen](#) auf Seite 144

# Adressdaten einer Website

Auf dem Tabreiter **Adressen** werden die folgende Adressdaten abgebildet.

**Tabelle 17: Adressdaten einer Website**

Eigenschaften	Beschreibung
Präfix	Eindeutige Kennung des Präfixes der Websitesammlung, unterhalb der die Website angelegt werden soll. Ein Wert wird nur angezeigt, wenn die Website über den One Identity Manager angelegt wurde.

Eigenschaften	Beschreibung
URL relativ zum Server	URL der Website, relativ zur URL der Webanwendung.
URL	Absolute URL der Website.
URL der Systemgestaltungsvorlage	URL zur Systemgestaltungsvorlage, relativ zur URL der Webanwendung.
URL der Gestaltungsvorlage der Website	URL zur Gestaltungsvorlage der Website, relativ zur URL der Webanwendung.
URL des Portals	URL zu einer Portalwebsite, mit der die Website verknüpft ist.

Wenn der in der URL benannte Server per DNS aufgelöst werden kann, können Sie die Website im Standardbrowser öffnen.

### Um die Website zu öffnen

1. Wählen Sie die Kategorie **SharePoint | Websites**.
2. Wählen Sie in der Ergebnisliste die Website.
3. Wählen Sie die Aufgabe **URL öffnen**.

### Verwandte Themen

- [Einrichten von SharePoint Websitesammlungen und Websites](#) auf Seite 94

## Designinformationen einer Website

Auf dem Tabreiter **Design** werden die folgende Designinformationen abgebildet.

**Tabelle 18: Designinformationen einer Website**

Eigenschaft	Beschreibung
Webvorlage	Eindeutige Kennung der Webvorlage, die beim Erstellen der Website genutzt werden soll. Ein Wert wird nur angezeigt, wenn die Website über den One Identity Manager angelegt wurde.
Titel	Bezeichnung, unter der die Website angezeigt wird.
URL zum Logo	URL zum Logo der Website, relativ zur URL der Webanwendung.

Eigenschaft	Beschreibung
Beschreibung zum Logo-Icon	Beschreibung zum Logo der Website.

## Verwandte Themen

- [Einrichten von SharePoint Websitesammlungen und Websites](#) auf Seite 94

# Zusätzliche Aufgaben zur Verwaltung von Websites

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

Auf dem Überblicksformular werden alle für die Website zugelassenen Rollen und Berechtigungsstufen dargestellt. Über die Aufgabe **URL öffnen** können Sie die Website im Standardbrowser öffnen. Voraussetzung dafür ist, dass der in der URL benannte Server per DNS aufgelöst werden kann.

## Um einen Überblick über eine Website zu erhalten

1. Wählen Sie die Kategorie **SharePoint | Websites**.
2. Wählen Sie in der Ergebnisliste die Website.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Website**.

## Verwandte Themen

- [Adressdaten einer Website](#) auf Seite 91

# Vererbung von Berechtigungen an untergeordnete Websites

SharePoint Rollen werden auf der Ebene von Websites definiert. Für die Root-Site einer Websitesammlung sind immer Rollen definiert. Untergeordnete Websites können diese Rollendefinitionen erben. Ebenso werden Rollen auf der Root-Site einer Websitesammlung an Gruppen oder Benutzerkonten zugewiesen. Auch diese Zuweisungen können untergeordnete Websites erben. Über die Option **Eigene Rollendefinitionen** ist festgelegt, ob eine Website die Rollen von der übergeordneten Website erbt. Über die Optionen **Eigenen Rollenzuweisungen** ist festgelegt, ob Benutzerkonten und Gruppen auf eine Website explizit berechtigt werden können oder ob die Rollenzuweisungen von der übergeordneten Website geerbt werden.

## Detaillierte Informationen zum Thema

- [SharePoint Rollen und Gruppen](#) auf Seite 123

## Verwandte Themen

- [Allgemeine Stammdaten einer Website](#) auf Seite 90

# Einrichten von SharePoint Websitesammlungen und Websites

Websitesammlungen und Websites werden in der Standardinstallation des One Identity Manager durch die Synchronisation in die One Identity Manager-Datenbank lediglich eingelesen. Über unternehmensspezifische Anpassungen ist es möglich, Websitesammlungen und Websites im One Identity Manager neu anzulegen und in die SharePoint-Umgebung zu publizieren. Zu diesem Zweck werden die Spalten `UID_SPSPrefix` und `UID_SPSPWebTemplate` an der Tabelle `SPSPWeb` sowie vordefinierte Skripte und Prozesse bereitgestellt.

**HINWEIS:** Folgende Skripte und Prozesse können Sie nutzen, um Websitesammlungen und Websites über den IT Shop bestellbar zu machen. Passen Sie diese Skripte und Prozesse in jedem Fall unternehmensspezifisch an!

Skript/Prozess	Beschreibung
Skript VI_ CreateSPSSite	Erstellt eine neue Websitesammlung und die zugehörige Root-Site in der One Identity Manager-Datenbank. Erzeugt ein Benutzerkonto, das als Administrator der Websitesammlung bzw. Autor der Root-Site eingetragen wird.
Skript VI_ CreateSPSPWeb	Erstellt eine neue Website innerhalb einer Websitesammlung in der One Identity Manager-Datenbank.
Prozess SP0_ SPSPWeb_ (De-)Provision	Erstellt eine neue Website innerhalb einer Websitesammlung. Der Prozess wird durch das Ereignis <code>PROVISION</code> ausgelöst, wenn die Website in der One Identity Manager-Datenbank nicht als Root-Site gekennzeichnet ist.
Prozess SP0_ SPSPSite_ (De-)Provision	Erstellt eine neue Websitesammlung innerhalb einer Webanwendung und die zugehörige Root-Site. Der Prozess wird durch das Ereignis <code>PROVISION</code> ausgelöst.

Folgende Schritte sind darüber hinaus erforderlich:

- Definieren Sie ein bestellbares Produkt, über das die Websitesammlung/Website im IT Shop bestellt wird.

- Definieren Sie Produkteigenschaften, die auf die Skriptparameter gemappt werden (beispielsweise Webanwendung, Präfix oder Webvorlage). Diese Produkteigenschaften müssen bei der Bestellung der Websitesammlung/Website erfasst werden.
- Erstellen Sie einen Prozess für die Tabelle PersonWantsOrg, der ausgelöst wird, wenn die Bestellung genehmigt wurde (Ereignis OrderGranted). Der Prozess ruft das passende Skript auf und besetzt dessen Parameterwerte mit den definierten Produkteigenschaften. Dadurch wird die Websitesammlung/Website in der One Identity Manager-Datenbank angelegt.

## SharePoint Benutzerkonten

SharePoint Benutzerkonten halten die zur Authentifizierung eines Benutzers notwendigen Informationen vor, wie beispielsweise den Authentifizierungsmodus und den Anmeldenamen. Des Weiteren sind an den Benutzerkonten die Berechtigungen der Benutzer innerhalb einer Websitesammlung festgelegt.

Jedes SharePoint Benutzerkonto repräsentiert ein Objekt aus einem Authentifizierungssystem, dem die SharePoint-Installation vertraut. Wenn dieses Authentifizierungssystem als Zielsystem im One Identity Manager verwaltet wird, kann das zur Authentifizierung genutzte Objekt am SharePoint Benutzerkonto als Authentifizierungsobjekt hinterlegt werden. Damit können die Berechtigungen der SharePoint Benutzerkonten auf die im One Identity Manager verwalteten Identitäten abgebildet werden. Der One Identity Manager schafft damit die Möglichkeit, einen Überblick über alle SharePoint Zugriffsberechtigungen einer Identität zu erhalten. SharePoint Berechtigungen können attestiert und Complianceprüfungen durchgeführt werden. Bei entsprechender Konfiguration können Mitarbeiter ihre benötigten SharePoint Berechtigungen über ihre Mitgliedschaften in hierarchischen Rolle erhalten oder über das Web Portal bestellen.

### Beispiel

Für eine Websitesammlung soll ein Gastzugang eingerichtet werden, der nur zum Lesen berechtigt. Dafür wird ein SharePoint Benutzerkonto angelegt. Diesem Benutzerkonto wird als Authentifizierungsobjekt die Active Directory Gruppe "Guests" zugeordnet. Clara Harris besitzt ein Active Directory Benutzerkonto, das Mitglied dieser Gruppe ist. Damit kann sie sich an der Websitesammlung anmelden und erhält alle Berechtigungen des SharePoint Benutzerkontos.

Jan Bloggs soll ebenfalls einen Gastzugang für die Websitesammlung erhalten. Er besitzt ein Active Directory Benutzerkonto in der selben Domäne. Im Web Portal bestellt er die Mitgliedschaft in der Active Directory Gruppe "Guests". Sobald die Bestellung genehmigt und zugewiesen ist, kann er sich an der Websitesammlung anmelden.

Standardmäßig können im One Identity Manager folgende Objekte als Authentifizierungsobjekte zugeordnet werden:



- Active Directory Gruppen (ADSGroup)
- Active Directory Benutzerkonten (ADSAccount)
- LDAP Gruppen (LDAPGroup)
- LDAP Benutzerkonten (LDAPAccount)

Bei der Synchronisation versucht der One Identity Manager anhand des Anmeldenamens das passende Authentifizierungsobjekt zuzuordnen.

Abhängig vom referenzierten Authentifizierungsobjekt werden SharePoint Zugriffsberechtigungen im One Identity Manager auf unterschiedliche Weise bereitgestellt.

### **Fall 1: Das Authentifizierungsobjekt ist eine Gruppe. Das Authentifizierungssystem wird im One Identity Manager verwaltet. (Standardfall)**

- Das Benutzerkonto repräsentiert eine Active Directory oder LDAP Gruppe. Diese Gruppe kann im One Identity Manager als Authentifizierungsobjekt zugeordnet werden.
- Dem Benutzerkonto kann keine Identität zugeordnet werden. Damit kann das Benutzerkonto nur über Direktzuweisung Mitglied in SharePoint Rollen und Gruppen werden.
- Damit sich eine Identität am SharePoint-System anmelden kann, benötigt sie ein Active Directory oder LDAP Benutzerkonto. Dieses Benutzerkonto muss Mitglied in der als Authentifizierungsobjekt genutzten Active Directory oder LDAP Gruppe sein.
- Ein neues SharePoint Benutzerkonto kann manuell erstellt werden.
- Das Benutzerkonto kann nicht über eine Kontendefinition verwaltet werden.

### **Fall 2: Das Authentifizierungsobjekt ist ein Benutzerkonto. Das Authentifizierungssystem wird im One Identity Manager verwaltet.**

- Das Benutzerkonto repräsentiert ein Active Directory oder LDAP Benutzerkonto. Dieses Benutzerkonto kann im One Identity Manager als Authentifizierungsobjekt zugeordnet werden.
- Dem SharePoint Benutzerkonto kann eine Identität zugeordnet werden. Damit kann das Benutzerkonto über Vererbung und über Direktzuweisung Mitglied in SharePoint Rollen und Gruppen werden.

Wenn ein Authentifizierungsobjekt zugeordnet ist, wird die verbundene Identität über das Authentifizierungsobjekt ermittelt.

Wenn kein Authentifizierungsobjekt zugeordnet ist, kann die Identität automatisch oder manuell zugeordnet werden. Die automatische Identitätenzuordnung ist abhängig von den Konfigurationsparametern **TargetSystem | SharePoint | PersonAutoFullsync** und **TargetSystem | SharePoint | PersonAutoDefault**.

- Ein neues SharePoint Benutzerkonto kann manuell oder über eine Kontendefinition erstellt werden. Das Active Directory oder LDAP Benutzerkonto, das als

Authentifizierungsobjekt genutzt wird, muss zu einer Domäne gehören dem das referenzierte Authentifizierungssystem vertraut.

- Das Benutzerkonto kann über eine Kontendefinition verwaltet werden.

### **Fall 3: Das Authentifizierungsobjekt ist ein Benutzerkonto. Das Authentifizierungssystem wird nicht im One Identity Manager verwaltet.**

- Dem Benutzerkonto kann kein Authentifizierungsobjekt zugeordnet werden.
- Dem Benutzerkonto kann eine Identität manuell oder automatisch zugeordnet werden. Damit kann das Benutzerkonto über Vererbung und über Direktzuweisung Mitglied in SharePoint Rollen und Gruppen werden. Die automatische Identitätenzuordnung ist abhängig von den Konfigurationsparametern **TargetSystem | SharePoint | PersonAutoFullsync** und **TargetSystem | SharePoint | PersonAutoDefault**.
- Ein neues SharePoint Benutzerkonto kann manuell oder über eine Kontendefinition erstellt werden. Wenn eine Kontendefinition verwendet wird, müssen die Bildungsregeln für die Spalten `SPSUser.LoginName` und `SPSUser.DisplayName` kundenspezifisch angepasst werden.
- Das Benutzerkonto kann über eine Kontendefinition verwaltet werden.

Die Grundlagen zur Verwaltung von Identitäten und Benutzerkonten sind im One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul beschrieben.

## **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.

- Identitätstyp

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

**Tabelle 19: Identitätstypen von Benutzerkonten**

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

- Privilegiertes Benutzerkonto

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

## Standardbenutzerkonten

In der Regel erhält jede Identität ein Standardbenutzerkonto, das die Berechtigungen besitzt, die für die tägliche Arbeit benötigt werden. Die Benutzerkonten haben eine Verbindung zur Identität. Die Verbindung zwischen Identität und SharePoint Benutzerkonto wird standardmäßig über das Authentifizierungsobjekt hergestellt, das dem Benutzerkonto zugeordnet ist. Davon abweichend können Identitäten auch direkt mit den Benutzerkonten verbunden sein. Solche Benutzerkonten können über Kontendefinitionen verwaltet werden. Über eine Kontendefinition und deren Automatisierungsgrade kann die Auswirkung der Verbindung und der Umfang der vererbten Eigenschaften der Identität 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 Identität 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 Identität ermittelt werden können.

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

- Verwenden Sie in den Abbildungsvorschriften für die Spalten `IsGroupAccount_SPSGroup` und `IsGroupAccount_SPSRLAsgn` 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 Identitäten zu.  
  
Durch die Zuweisung der Kontendefinition an eine Identität wird über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

## Administrative Benutzerkonten

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

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

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

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

- Persönliche Administratoridentität
  1. Verbinden Sie das Benutzerkonto über die Spalte UID\_Person mit einer Identität.  
Nutzen Sie eine Identität mit demselben Identitätstyp oder erstellen Sie eine neue Identität.
  2. Weisen Sie diese Identität an hierarchische Rollen zu.
- Gruppenidentität
  1. Weisen Sie dem Benutzerkonto alle Identitäten mit Nutzungsberechtigungen zu.
  2. Verbinden Sie das Benutzerkonto über die Spalte UID\_Person mit einer Pseudo-Identität.  
Nutzen Sie eine Identität mit demselben Identitätstyp oder erstellen Sie eine neue Identität.
  3. Weisen Sie diese Pseudo-Identität an hierarchische Rollen zu.

Das Benutzerkonto erhält seine Berechtigungen über die Pseudo-Identität.

## Privilegierte Benutzerkonten

Privilegierte Benutzerkonten werden eingesetzt, um Identitäten 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 Identität 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 Identität 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, dass privilegierte Benutzerkonten die Berechtigungen des Standardbenutzers erben, definieren Sie eine Abbildungsvorschriften für die Spalten `IsGroupAccount_SPSGroup` und `IsGroupAccount_SPSRLAsgn` 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 Identitäten zu, die mit privilegierten Benutzerkonten arbeiten sollen.

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


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

## Erfassen der Stammdaten für SharePoint Benutzerkonten


Jedes SharePoint Benutzerkonto repräsentiert ein Objekt aus einem Authentifizierungssystem. Dieses Objekt kann eine Gruppe oder ein Benutzer sein. In der Navigationsansicht können die gruppenthentifizierten und die benutzenthentifizierten Benutzerkonten separat ausgewählt werden.

### ***Um die Stammdaten eines gruppenthentifizierten Benutzerkontos zu bearbeiten***

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (gruppenthentifiziert)**.

2. Wählen Sie in der Ergebnisliste das Benutzerkonto und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.  
- ODER -  
Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

#### ***Um die Stammdaten eines benutzerauthentifizierten Benutzerkontos zu bearbeiten***

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.  
- ODER -  
Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

#### ***Um ein benutzerauthentifiziertes Benutzerkonto für eine Identität manuell zuzuweisen oder zu erstellen***

1. Wählen Sie die Kategorie **Identitäten | Identitäten**.
2. Wählen Sie in der Ergebnisliste die Identität aus und führen Sie die Aufgabe **SharePoint Benutzerkonten zuweisen** aus.
3. Weisen Sie ein Benutzerkonto zu.
4. Speichern Sie die Änderungen.


#### **Detaillierte Informationen zum Thema**

- [Stammdaten eines gruppenauthentifizierten Benutzerkontos](#) auf Seite 103
- [Stammdaten eines benutzerauthentifizierten Benutzerkontos](#) auf Seite 107

## **Stammdaten eines gruppenauthentifizierten Benutzerkontos**

Für ein gruppenauthentifiziertes Benutzerkonto erfassen Sie die folgenden Stammdaten.

**Tabelle 20: Stammdaten eines gruppenthentifizierten Benutzerkontos**

<b>Eigenschaft</b>	<b>Beschreibung</b>
Identität	<p>Identität, die das Benutzerkonto verwendet.</p> <ul style="list-style-type: none"> <li>• Wurde das Benutzerkonto über eine Kontendefinition erzeugt, ist die Identität bereits eingetragen.</li> <li>• Wenn Sie die automatische Identitätenzuordnung nutzen, wird beim Speichern des Benutzerkontos eine zugehörige Identität gesucht und in das Benutzerkonto übernommen.</li> <li>• Wenn Sie das Benutzerkonto manuell erstellen, können Sie die Identität aus der Auswahlliste wählen.</li> </ul> <p>In der Auswahlliste werden im Standard aktivierte und deaktivierte Identitäten angezeigt. Um deaktivierte Identitäten nicht in der Auswahlliste anzuzeigen, aktivieren Sie den Konfigurationsparameter <b>QER   Person   HideDeactivatedIdentities</b>.</p> <p><b>HINWEIS:</b> Wenn Sie eine deaktivierte Identität an ein Benutzerkonto zuordnen, wird das Benutzerkonto, abhängig von der Konfiguration, unter Umständen gesperrt oder gelöscht.</p> <p>Wenn ein Authentifizierungsobjekt zugeordnet ist, wird die verbundene Identität per Bildungsregel über das Authentifizierungsobjekt ermittelt. Wenn kein Authentifizierungsobjekt zugeordnet ist, kann die Identität automatisch oder manuell zugeordnet werden.</p> <p>Für ein Benutzerkonto mit einer Identität vom Typ <b>Organisatorische Identität, Persönliche Administratoridentität, Zusatzidentität, Gruppenidentität</b> oder <b>Dienstidentität</b> können Sie eine neue Identität erstellen. Klicken Sie dafür  neben dem Eingabefeld und erfassen Sie die erforderlichen Identitätenstammdaten. Die Pflichteingaben sind abhängig vom gewählten Identitätstyp.</p>
Keine Verbindung mit einer Identität erforderlich	<p>Gibt an, ob dem Benutzerkonto absichtlich keine Identität zugeordnet ist. Sie können die Option manuell setzen. Aktivieren Sie die Option, falls das Benutzerkonto mit keiner Identität verbunden werden muss (beispielsweise, wenn mehrere Identitäten das Benutzerkonto verwenden).</p> <p>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 Identität</p>



Eigenschaft	Beschreibung
	verbunden sind, nach verschiedenen Kriterien gefiltert werden.
Nicht mit einer Identität verbunden	Zeigt an, warum für das Benutzerkonto die Option <b>Keine Verbindung mit einer Identität erforderlich</b> aktiviert ist. Das Benutzerkonto wird aufgrund eines Ausschlusskriteriums nicht mit einer Identität verbunden.
Websitesammlung	Websitesammlung, in der das Benutzerkonto genutzt wird.
Gruppenauthentifiziert	Angabe, ob das Authentifizierungsobjekt des Benutzerkontos eine Gruppe ist.
Authentifizierungsobjekt	<p>Authentifizierungsobjekt, welches das Benutzerkonto referenziert. Jedes SharePoint Benutzerkonto repräsentiert ein Objekt aus einem Authentifizierungssystem, dem die SharePoint-Installation vertraut. Wenn dieses Authentifizierungssystem als Zielsystem im One Identity Manager verwaltet wird, kann das zur Authentifizierung genutzte Objekt am SharePoint Benutzerkonto als Authentifizierungsobjekt hinterlegt werden.</p> <p>Das Authentifizierungsobjekt wird bei der Synchronisation automatisch zugeordnet. Beim Einrichten eines neuen Benutzerkontos im Manager, können sie ein Authentifizierungsobjekt zuordnen. Nach dem Speichern kann das Authentifizierungsobjekt nicht mehr geändert werden.</p> <p>Einem gruppenauthentifizierten Benutzerkonto können folgende Authentifizierungsobjekte zugeordnet werden:</p> <ul style="list-style-type: none"> <li>• Active Directory Gruppen mit dem Gruppentyp „Sicherheitsgruppe“ aus der Domäne, die der Farm zugeordnet ist, oder einer Domäne in Vertrauensstellung</li> <li>• LDAP Gruppen aus der Domäne, die der Farm zugeordnet ist</li> </ul>
Authentifizierungsmodus	<p>Authentifizierungsmodus, der bei der Anmeldung mit diesem Benutzerkonto am SharePoint Server genutzt wird.</p> <p>Der Anmeldenamen neuer Benutzerkonten ist abhängig vom verwendeten Authentifizierungsmodus. Der Authentifizierungsmodus wird durch eine Bildungsregel gesetzt. Der Wert ist abhängig von der Option <b>Forderungsauthentifizierung</b> der zugehörigen Webanwendung. Wenn Sie unternehmensspezifische Authentifizierungsmodi definiert haben, wählen Sie den Authentifizierungsmodus aus der Auswahlliste aus.</p>

Eigenschaft	Beschreibung
	<b>HINWEIS:</b> Damit ein unternehmensspezifisch angelegter Authentifizierungsmodus an Benutzerkonten zugeordnet werden kann, passen Sie die Bildungsregel für diese Spalte unternehmensspezifisch an ( <code>SPSUser.UID_SPSAuthSystem</code> ).
Anzeigename	Beliebiger Anzeigename des Benutzerkontos. Wird standardmäßig aus dem Anzeigenamen des Authentifizierungsobjektes gebildet. Wenn kein Authentifizierungsobjekt zugeordnet ist, tragen Sie den Anzeigenamen manuell ein.
Anmeldename	Anmeldename des Benutzerkontos. Er wird über eine Bildungsregeln ermittelt. Wenn kein Authentifizierungsobjekt zugeordnet ist, tragen Sie den Anmeldenenamen manuell ein. <b>HINWEIS:</b> Damit ein Anmeldename gebildet werden kann, wenn ein unternehmensspezifischer Authentifizierungsmodus zugeordnet ist, passen Sie die Bildungsregel für diese Spalte unternehmensspezifisch an ( <code>SPSUser.LoginName</code> ).
E-Mail-Adresse	E-Mail-Adresse des Benutzerkontos. Sie wird über Bildungsregeln aus der E-Mail-Adresse des Authentifizierungsobjektes gebildet.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten SharePoint Rollen und Gruppen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter <b>QER   CalculateRiskIndex</b> aktiviert ist. Ausführliche Informationen finden Sie im <i>One Identity Manager Administrationshandbuch für Risikobewertungen</i> .
Kategorie	Kategorien für die Vererbung von Gruppen an das Benutzerkonto. Gruppen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Hinweise	Freitextfeld für zusätzliche Erläuterungen.
Identitätstyp	Typ der Identität des Benutzerkontos. Zulässige Werte sind: <ul style="list-style-type: none"> <li>• <b>Primäre Identität:</b> Standardbenutzerkonto einer Identität.</li> <li>• <b>Organisatorische Identität:</b> Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen.</li> </ul>

Eigenschaft	Beschreibung
	<ul style="list-style-type: none"> <li>• <b>Persönliche Administratoridentität:</b> Benutzerkonto mit administrativen Berechtigungen, welches von einer Identität genutzt wird.</li> <li>• <b>Zusatzidentität:</b> Benutzerkonto, das für einen spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken.</li> <li>• <b>Gruppenidentität:</b> Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Identitäten genutzt wird. Weisen Sie alle Identitäten zu, die das Benutzerkonto nutzen.</li> <li>• <b>Dienstidentität:</b> Dienstkonto.</li> </ul>
Privilegiertes Benutzerkonto	Angabe, ob es sich um ein privilegiertes Benutzerkonto handelt.
Administrator	Angabe, ob das Benutzerkonto Administrator einer Websitesammlung ist.
Auditor	Angabe, ob das Benutzerkonto Auditor einer Websitesammlung ist.

## Detaillierte Informationen zum Thema


- [Authentifizierungsmodi](#) auf Seite 51
- [Festlegen der Kategorien für die Vererbung von SharePoint Gruppen](#) auf Seite 89
- [Unterstützte Typen von Benutzerkonten](#) auf Seite 98
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

# Stammdaten eines benutzerauthentifizierten Benutzerkontos

Für ein benutzerauthentifiziertes Benutzerkonto erfassen Sie die folgenden Stammdaten.

**Tabelle 21: Stammdaten eines benutzerauthentifizierten Benutzerkontos**

Eigenschaft	Beschreibung
Identität	<p>Identität, die das Benutzerkonto verwendet.</p> <ul style="list-style-type: none"> <li>• Wurde das Benutzerkonto über eine Kontendefinition erzeugt, ist die Identität bereits eingetragen.</li> <li>• Wenn Sie die automatische Identitätenzuordnung</li> </ul>

Eigenschaft	Beschreibung
	<p>nutzen, wird beim Speichern des Benutzerkontos eine zugehörige Identität gesucht und in das Benutzerkonto übernommen.</p> <ul style="list-style-type: none"> <li>• Wenn Sie das Benutzerkonto manuell erstellen, können Sie die Identität aus der Auswahlliste wählen.</li> </ul> <p>In der Auswahlliste werden im Standard aktivierte und deaktivierte Identitäten angezeigt. Um deaktivierte Identitäten nicht in der Auswahlliste anzuzeigen, aktivieren Sie den Konfigurationsparameter <b>QER   Person   HideDeactivatedIdentities</b>.</p> <p><b>HINWEIS:</b> Wenn Sie eine deaktivierte Identität an ein Benutzerkonto zuordnen, wird das Benutzerkonto, abhängig von der Konfiguration, unter Umständen gesperrt oder gelöscht.</p> <p>Wenn ein Authentifizierungsobjekt zugeordnet ist, wird die verbundene Identität per Bildungsregel über das Authentifizierungsobjekt ermittelt. Wenn kein Authentifizierungsobjekt zugeordnet ist, kann die Identität automatisch oder manuell zugeordnet werden.</p> <p>Für ein Benutzerkonto mit einer Identität vom Typ <b>Organisatorische Identität, Persönliche Administratoridentität, Zusatzidentität, Gruppenidentität</b> oder <b>Dienstidentität</b> können Sie eine neue Identität erstellen. Klicken Sie dafür  neben dem Eingabefeld und erfassen Sie die erforderlichen Identitätenstammdaten. Die Pflichteingaben sind abhängig vom gewählten Identitätstyp.</p>
Keine Verbindung mit einer Identität erforderlich	<p>Gibt an, ob dem Benutzerkonto absichtlich keine Identität zugeordnet ist. Die Option wird automatisch aktiviert, wenn ein Benutzerkonto in der Ausschlussliste für die automatische Identitätenzuordnung enthalten ist oder eine entsprechende Attestierung erfolgt ist. Sie können die Option manuell setzen. Aktivieren Sie die Option, falls das Benutzerkonto mit keiner Identität verbunden werden muss (beispielsweise, wenn mehrere Identitäten das Benutzerkonto verwenden).</p> <p>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 Identität verbunden sind, nach verschiedenen Kriterien gefiltert werden.</p>

Eigenschaft	Beschreibung
Nicht mit einer Identität verbunden	<p>Zeigt an, warum für das Benutzerkonto die Option <b>Keine Verbindung mit einer Identität erforderlich</b> aktiviert ist. Mögliche Werte sind:</p> <ul style="list-style-type: none"> <li>• <b>durch Administrator:</b> Die Option wurde manuell durch den Administrator aktiviert.</li> <li>• <b>durch Attestierung:</b> Das Benutzerkonto wurde attestiert.</li> <li>• <b>durch Ausschlusskriterium:</b> Das Benutzerkonto wird aufgrund eines Ausschlusskriteriums nicht mit einer Identität verbunden. Das Benutzerkonto ist beispielsweise in der Ausschlussliste für die automatische Identitätenzuordnung enthalten (Konfigurationsparameter <b>PersonExcludeList</b>).</li> </ul>
Automatisierungsgrad	<p>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.</p>
Kontendefinition	<p>Kontendefinition, über die das Benutzerkonto erstellt wurde.</p> <p>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 Identität und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein.</p> <p><b>HINWEIS:</b> Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden.</p> <p><b>HINWEIS:</b> Über die Aufgabe <b>Entferne Kontendefinition</b> am Benutzerkonto können Sie das Benutzerkonto wieder in den Zustand <b>Linked</b> zurücksetzen. Dabei wird die Kontendefinition vom Benutzerkonto und von der Identität 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).</p> <p><b>HINWEIS:</b> Sollen Identitäten ihre SharePoint Benutzerkonten über Kontendefinitionen erhalten, müssen die Identitäten Benutzerkonten in der Active Directory Domäne oder LDAP Domäne besitzen, die an der SharePoint Farm hinterlegt ist, in der die SharePoint Benut-</p>

Eigenschaft	Beschreibung
	<p>zerkonten erstellt werden sollen.</p>
Websitesammlung	Websitesammlung, in der das Benutzerkonto genutzt wird.
Gruppenauthentifiziert	Angabe, ob das Authentifizierungsobjekt des Benutzerkontos eine Gruppe ist. Die Option ist bei benutzerauthentifizierten Benutzerkonten deaktiviert.
Authentifizierungsobjekt	<p>Authentifizierungsobjekt, welches das Benutzerkonto referenziert. Jedes SharePoint Benutzerkonto repräsentiert ein Objekt aus einem Authentifizierungssystem, dem die SharePoint-Installation vertraut. Wenn dieses Authentifizierungssystem als Zielsystem im One Identity Manager verwaltet wird, kann das zur Authentifizierung genutzte Objekt am SharePoint Benutzerkonto als Authentifizierungsobjekt hinterlegt werden.</p> <p>Das Authentifizierungsobjekt wird bei der Synchronisation automatisch zugeordnet. Beim Einrichten eines neuen Benutzerkontos im Manager, können sie ein Authentifizierungsobjekt zuordnen. Nach dem Speichern kann das Authentifizierungsobjekt nicht mehr geändert werden.</p> <p>Einem benutzerauthentifizierten Benutzerkonto können folgende Authentifizierungsobjekte zugeordnet werden:</p> <ul style="list-style-type: none"> <li>• Active Directory Benutzerkonten aus der Domäne, die der Farm zugeordnet ist, oder einer Domäne in Vertrauensstellung</li> <li>• LDAP Benutzerkonten aus der Domäne, die der Farm zugeordnet ist</li> </ul> <p>Benutzerkonten, die sich auf die Standard-SIDs einer Active Directory Umgebung beziehen, können im One Identity Manager kein Authentifizierungsobjekt referenzieren.</p> <p><b>HINWEIS:</b> Das SharePoint Benutzerkonto wird auch dann erstellt, wenn das Benutzerkonto, das als Authentifizierungsobjekt genutzt wird, deaktiviert oder gesperrt ist.</p>
Authentifizierungsmodus	<p>Authentifizierungsmodus, der bei der Anmeldung mit diesem Benutzerkonto am SharePoint Server genutzt wird.</p> <p>Der Anmeldename neuer Benutzerkonten ist abhängig vom verwendeten Authentifizierungsmodus. Der Authentifizierungsmodus wird durch eine Bildungsregel gesetzt. Der Wert ist abhängig von der Option</p>

Eigenschaft	Beschreibung
	<p><b>Forderungsauthentifizierung</b> der zugehörigen Webanwendung. Wenn Sie unternehmensspezifische Authentifizierungsmodi definiert haben, wählen Sie den Authentifizierungsmodus aus der Auswahlliste aus.</p> <p><b>HINWEIS:</b> Damit ein unternehmensspezifisch angelegter Authentifizierungsmodus an Benutzerkonten zugeordnet werden kann, passen Sie die Bildungsregel für diese Spalte unternehmensspezifisch an (<code>SPSUser.UID_SPSAuthSystem</code>).</p>
Anzeigename	Beliebiger Anzeigename des Benutzerkontos. Wird standardmäßig aus dem Anzeigenamen des Authentifizierungsobjektes gebildet. Wenn kein Authentifizierungsobjekt zugeordnet ist, tragen Sie den Anzeigenamen manuell ein.
Anmeldename	<p>Anmeldename des Benutzerkontos. Er wird über eine Bildungsregeln ermittelt. Wenn kein Authentifizierungsobjekt zugeordnet ist, tragen Sie den Anmeldenamen manuell ein.</p> <p><b>HINWEIS:</b> Damit ein Anmeldename gebildet werden kann, wenn ein unternehmensspezifischer Authentifizierungsmodus zugeordnet ist, passen Sie die Bildungsregel für diese Spalte unternehmensspezifisch an (<code>SPSUser.LoginName</code>).</p>
E-Mail-Adresse	E-Mail-Adresse des Benutzerkontos. Sie wird über Bildungsregeln aus der E-Mail-Adresse des Authentifizierungsobjektes gebildet.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten SharePoint Rollen und Gruppen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter <b>QER   CalculateRiskIndex</b> aktiviert ist. Ausführliche Informationen finden Sie im <i>One Identity Manager Administrationshandbuch für Risikobewertungen</i> .
Kategorie	Kategorien für die Vererbung von Gruppen an das Benutzerkonto. Gruppen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Hinweise	Freitextfeld für zusätzliche Erläuterungen.
Identitätstyp	<p>Typ der Identität des Benutzerkontos. Zulässige Werte sind:</p> <ul style="list-style-type: none"> <li>• <b>Primäre Identität:</b> Standardbenutzerkonto einer Identität.</li> </ul>

Eigenschaft	Beschreibung
	<ul style="list-style-type: none"> <li>• <b>Organisatorische Identität:</b> Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen.</li> <li>• <b>Persönliche Administratoridentität:</b> Benutzerkonto mit administrativen Berechtigungen, welches von einer Identität genutzt wird.</li> <li>• <b>Zusatzidentität:</b> Benutzerkonto, das für einen spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken.</li> <li>• <b>Gruppenidentität:</b> Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Identitäten genutzt wird. Weisen Sie alle Identitäten zu, die das Benutzerkonto nutzen.</li> <li>• <b>Dienstidentität:</b> Dienstkonto.</li> </ul>
Privilegiertes Benutzerkonto	Gibt an, ob es sich um ein privilegiertes Benutzerkonto handelt.
Gruppen erbbar	<p>Gibt an, ob das Benutzerkonto Gruppen über die verbundene Identität erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt.</p> <ul style="list-style-type: none"> <li>• Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen.</li> <li>• Wenn eine Identität eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Identität diese Gruppe nur, wenn die Option aktiviert ist.</li> </ul>
Rollen erbbar	Gibt an, ob das Benutzerkonto SharePoint Rollen über die verbundene Identität erben darf. Ist die Option aktiviert, werden die Rollen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt.
Administrator	Angabe, ob das Benutzerkonto Administrator einer Websitesammlung ist.
Auditor	Angabe, ob das Benutzerkonto Auditor einer Websitesammlung ist.



## Detaillierte Informationen zum Thema

- [Einrichten von Kontendefinitionen](#) auf Seite 62
- [Authentifizierungsmodi](#) auf Seite 51
- [Festlegen der Kategorien für die Vererbung von SharePoint Gruppen](#) auf Seite 89
- [Automatische Zuordnung von Identitäten zu SharePoint Benutzerkonten](#) auf Seite 116
- [Unterstützte Typen von Benutzerkonten](#) auf Seite 98
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

# Zusätzliche Aufgaben zur Verwaltung von SharePoint Benutzerkonten

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

## Überblick über das SharePoint Benutzerkonto

### *Um einen Überblick über ein Benutzerkonto zu erhalten*

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (gruppenauthentifiziert)** oder **SharePoint | Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das SharePoint Benutzerkonto**.

## SharePoint Gruppen direkt an ein SharePoint Benutzerkonto zuweisen

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


Es können nur Gruppen aus der Websitesammlung zugewiesen werden, zu der das Benutzerkonto gehört. 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 die Kategorie **SharePoint | Benutzerkonten (gruppenauthentifiziert)** oder **SharePoint | Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

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

#### **Um eine Zuweisung zu entfernen**

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

### **Verwandte Themen**

- [SharePoint Rollen direkt an ein Benutzerkonto zuweisen](#) auf Seite 114
- [SharePoint Gruppen an SharePoint Benutzerkonten zuweisen](#) auf Seite 128

## **SharePoint Rollen direkt an ein Benutzerkonto zuweisen**

SharePoint Rollen können einem Benutzerkonto direkt oder indirekt zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Identität und der SharePoint Rollen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Identität ein SharePoint Benutzerkonto, werden die SharePoint Rollen der hierarchischen Rollen an dieses Benutzerkonto vererbt. An gruppenauthentifizierte Benutzerkonten können die SharePoint Rollen nur direkt zugewiesen werden.

Es können nur SharePoint Rollen aus der Websitesammlung zugewiesen werden, zu der das Benutzerkonto gehört. SharePoint Rollen, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

**HINWEIS:** SharePoint Rollen, die auf Berechtigungsstufen verweisen, bei denen die Option **Versteckt** aktiviert ist, können nicht an Benutzerkonten zugewiesen werden.

### **Um SharePoint Rollen direkt an ein Benutzerkonto zuzuweisen**

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (gruppenauthentifiziert)** oder **SharePoint | Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **SharePoint Rollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Rollen zu.  
- ODER -  
Entfernen Sie im Bereich **Zuordnungen entfernen** die Rollen.
5. Speichern Sie die Änderungen.

### **Verwandte Themen**

- [SharePoint Gruppen direkt an ein SharePoint Benutzerkonto zuweisen](#) auf Seite 113
- [Erfassen der Stammdaten für SharePoint Berechtigungsstufen](#) auf Seite 145

## **Zusatzeigenschaften zuweisen**

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

### **Um Zusatzeigenschaften für ein Benutzerkonto festzulegen**

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (gruppenauthentifiziert)** oder **SharePoint | Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.  
- ODER -  
Entfernen Sie im Bereich **Zuordnungen entfernen** die Zusatzeigenschaften.
5. Speichern Sie die Änderungen.

### **Detaillierte Informationen zum Thema**

- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

# Unternehmensspezifische Authentifizierungsmodi nutzen

Wenn Benutzerkonten angelegt werden, werden die Werte verschiedener Stammdaten durch Bildungsregeln ermittelt. Bei der Synchronisation versucht der One Identity Manager ein Authentifizierungsobjekt über die Eigenschaften des Benutzerkontos zu identifizieren und zuzuordnen. Um unternehmensspezifische Authentifizierungsmodi nutzen zu können, müssen die Bildungsregeln verschiedener Spalten gegebenenfalls angepasst werden. Erstellen Sie unternehmensspezifische Bildungsregeln, damit die Authentifizierungsmodi automatisch an Benutzerkonten zugeordnet werden können und Anmeldenames korrekt gebildet werden.

## **Um einen unternehmensspezifischen Authentifizierungsmodus zu nutzen**

1. Passen Sie im Designer die Bildungsregel für die Spalte `SPSUser.UID_SPSAuthSystem` (Authentifizierungsmodus) an.
2. Prüfen Sie die Bildungsregeln der Spalten `SPSUser.ObjectKeyNamespaceItem` (Authentifizierungsobjekt) und `SPSUser.LoginName` (Anmeldename) und passen Sie diese gegebenenfalls an.

## **Detaillierte Informationen zum Thema**

- [Authentifizierungsmodi](#) auf Seite 51
- One Identity Manager Konfigurationshandbuch

# Automatische Zuordnung von Identitäten zu SharePoint Benutzerkonten

**Tabelle 22: Konfigurationsparameter für die automatische Identitätenzuordnung**

Konfigurationsparameter	Bedeutung
TargetSystem   SharePoint   PersonAutoFullsync	Modus für die automatische Identitätenzuordnung für Benutzerkonten, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem   SharePoint   PersonAutoDefault	Modus für die automatische Identitätenzuordnung für Benutzerkonten, die außerhalb der Synchronisation in der Datenbank angelegt werden.

Beim Einfügen eines benutzerauthentifizierten Benutzerkontos kann automatisch eine vorhandene Identität zugeordnet werden. Dieser Mechanismus kann auf die Erstellung eines neuen Benutzerkontos durch manuelle Anlage oder Synchronisation folgen.

Für die automatische Identitätenzuordnung definieren Sie Kriterien für die Ermittlung der Identitäten. Wird durch den eingesetzten Modus ein Benutzerkonto mit einer Identität 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 Identitäten 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 Identitäten zu Benutzerkonten bleiben bestehen.

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

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

#### **Voraussetzungen:**

- An den Benutzerkonten ist die Option **Gruppenauthentifiziert** deaktiviert.
- Den Benutzerkonten ist kein Authentifizierungsobjekt zugeordnet.

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

- Wenn Identitäten bei der Synchronisation von Benutzerkonten zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | SharePoint | PersonAutoFullsync** und wählen Sie den gewünschte Modus aus.
- Wenn Identitäten außerhalb der Synchronisation zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | SharePoint | PersonAutoDefault** und wählen Sie den gewünschten Modus aus.
- Weisen Sie der Websitesammlung eine Kontendefinition zu. Stellen Sie sicher, dass der Automatisierungsgrad, der verwendet werden soll, als Standardautomatisierungsgrad eingetragen ist.
- Definieren Sie die Suchkriterien für die Identitätenzuordnung an der Websitesammlung.

#### **HINWEIS:**

Für die Synchronisation gilt:

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

Außerhalb der Synchronisation gilt:

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

## Verwandte Themen

- [Erstellen einer Kontendefinition](#) auf Seite 63
- [Zuweisen der Kontendefinition an ein Zielsystem](#) auf Seite 80
- [Bearbeiten der Suchkriterien für die automatische Identitätenzuordnung](#) auf Seite 118

# Bearbeiten der Suchkriterien für die automatische Identitätenzuordnung

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

Die Kriterien für die Identitätenzuordnung werden an der Websitesammlung definiert. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Identität übereinstimmen müssen, damit die Identität 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 Identitätenzuordnung** (AccountToPersonMatchingRule) der Tabelle SPSSite geschrieben.

Die Suchkriterien werden bei der automatischen Zuordnung von Identitäten zu Benutzerkonten ausgewertet. Darüber hinaus können Sie anhand der Suchkriterien eine Vorschlagsliste für die Identitätenzuordnung 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 Identitätenzuordnung festzulegen

1. Wählen Sie die Kategorie **SharePoint | Websitesammlungen**.
2. Wählen Sie in der Ergebnisliste die Websitesammlung.
3. Wählen Sie die Aufgabe **Suchkriterien für die Identitätenzuordnung definieren**.

- Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Identität übereinstimmen müssen, damit die Identität mit dem Benutzerkonto verbunden wird.

**Tabelle 23: Standardsuchkriterien für Benutzerkonten**

Anwenden auf	Spalte an Identität	Spalte am Benutzerkonto
Benutzerkonten (benutzerauthentifiziert)	Zentrales Benutzerkonto (CentralAccount)	Anmeldename (LoginName)

- Speichern Sie die Änderungen.

## Direkte Zuordnung von Identitäten an Benutzerkonten anhand einer Vorschlagsliste

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

**Tabelle 24: Ansichten zur manuellen Zuordnung**

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

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

### Um die Suchkriterien auf die Benutzerkonten anzuwenden

- Klicken Sie **Neu laden**.

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

### Um Identitäten direkt über die Vorschlagsliste zuzuordnen

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

Den ausgewählten Benutzerkonten werden die per Suchkriterium ermittelten Identitäten zugeordnet.
- ODER –
2. Klicken Sie **Ohne Identitätenzuordnung**.
  - a. Klicken Sie **Identität auswählen** für das Benutzerkonto, dem eine Identität zugeordnet werden soll. Wählen Sie eine Identität aus der Auswahlliste.
  - b. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die ausgewählten Identitäten zugeordnet werden sollen. Eine Mehrfachauswahl ist möglich.
  - c. Klicken Sie **Ausgewählte zuweisen**.
  - d. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Den ausgewählten Benutzerkonten werden die Identitäten zugeordnet, die in der Spalte **Identität** angezeigt werden.

### Um Zuordnungen zu entfernen

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


Von den ausgewählten Benutzerkonten werden die zugeordneten Identitäten entfernt.

## Löschen und Wiederherstellen von SharePoint Benutzerkonten


**HINWEIS:** Solange eine Kontendefinition für eine Identität wirksam ist, behält die Identität ihr daraus entstandenes Benutzerkonto. Wird die Zuweisung einer Kontendefinition entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht. Benutzerkonten, die als **Ausstehend** markiert sind, werden nur gelöscht, wenn der Konfigurationsparameter **QER | Person | User | DeleteOptions | DeleteOutstanding** aktiviert ist.



### Um ein Benutzerkonto zu löschen

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (gruppenauthentifiziert)** oder **SharePoint | Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie , um das Benutzerkonto zu löschen.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

### Um ein Benutzerkonto wiederherzustellen

1. Wählen Sie die Kategorie **SharePoint | Benutzerkonten (gruppenauthentifiziert)** oder **SharePoint | Benutzerkonten (benutzerauthentifiziert)**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste .

Wenn das Authentifizierungsobjekt, das einem SharePoint Benutzerkonto zugeordnet ist, aus der One Identity Manager-Datenbank gelöscht wird, wird der Verweis auf das Authentifizierungsobjekt vom SharePoint Benutzerkonto entfernt. Um dieses Benutzerkonten ebenfalls aus der One Identity Manager-Datenbank zu löschen, definieren Sie unternehmensspezifische Prozesse.

### Konfigurieren der Löschverzögerung

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 SPSUser 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 SPSUser ein **Skript (Löschverzögerung)**.

### Beispiel:

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

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

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

**HINWEIS:** SharePoint Benutzerkonten können nicht gesperrt werden. Ein Benutzerkonto, das zum Löschen markiert ist, bleibt solange aktiv, bis die Löscherzögerung abgelaufen und das Benutzerkonto endgültig aus der One Identity Manager-Datenbank gelöscht ist.

Sperren Sie das Benutzerkonto, das als Authentifizierungsobjekt mit dem SharePoint Benutzerkonto verbunden ist, um zu verhindern, dass sich ein Benutzer mit einem zum Löschen markierten SharePoint Benutzerkonto an einer Website anmeldet.

## SharePoint Rollen und Gruppen

SharePoint Berechtigungen werden über SharePoint Rollen und SharePoint Gruppen an Benutzerkonten vererbt. Dabei werden SharePoint Gruppen immer für eine Websitesammlung definiert. SharePoint Rollen werden für Websites definiert. Sie werden an Gruppen zugewiesen und vererben darüber die SharePoint Berechtigungen an die Benutzerkonten, die Mitglied dieser Gruppen sind. SharePoint Rollen können auch direkt an Benutzerkonten zugewiesen werden. Durch die zugewiesenen SharePoint Rollen werden die Berechtigungen der Benutzerkonten auf einzelne Websites einer Websitesammlung eingeschränkt.

### Begriffe

- Eine SharePoint Rolle ist die mit einer konkreten Website verknüpfte Berechtigungsstufe.
- Als Rollendefinition wird die Zuweisung von SharePoint Berechtigungen an eine Berechtigungsstufe bezeichnet.
- Die Zuweisung von Benutzerkonten oder Gruppen an eine SharePoint Rolle wird als Rollenzuweisung bezeichnet.

Websites können die Berechtigungen, die die Benutzerkonten auf die Website haben, an untergeordnete Websites vererben. Als übergeordnete Website gilt jede Root-Site einer Websitesammlung sowie jede Website, der eine weitere Website hierarchisch untergeordnet ist. Dabei sind folgende Szenarien möglich:

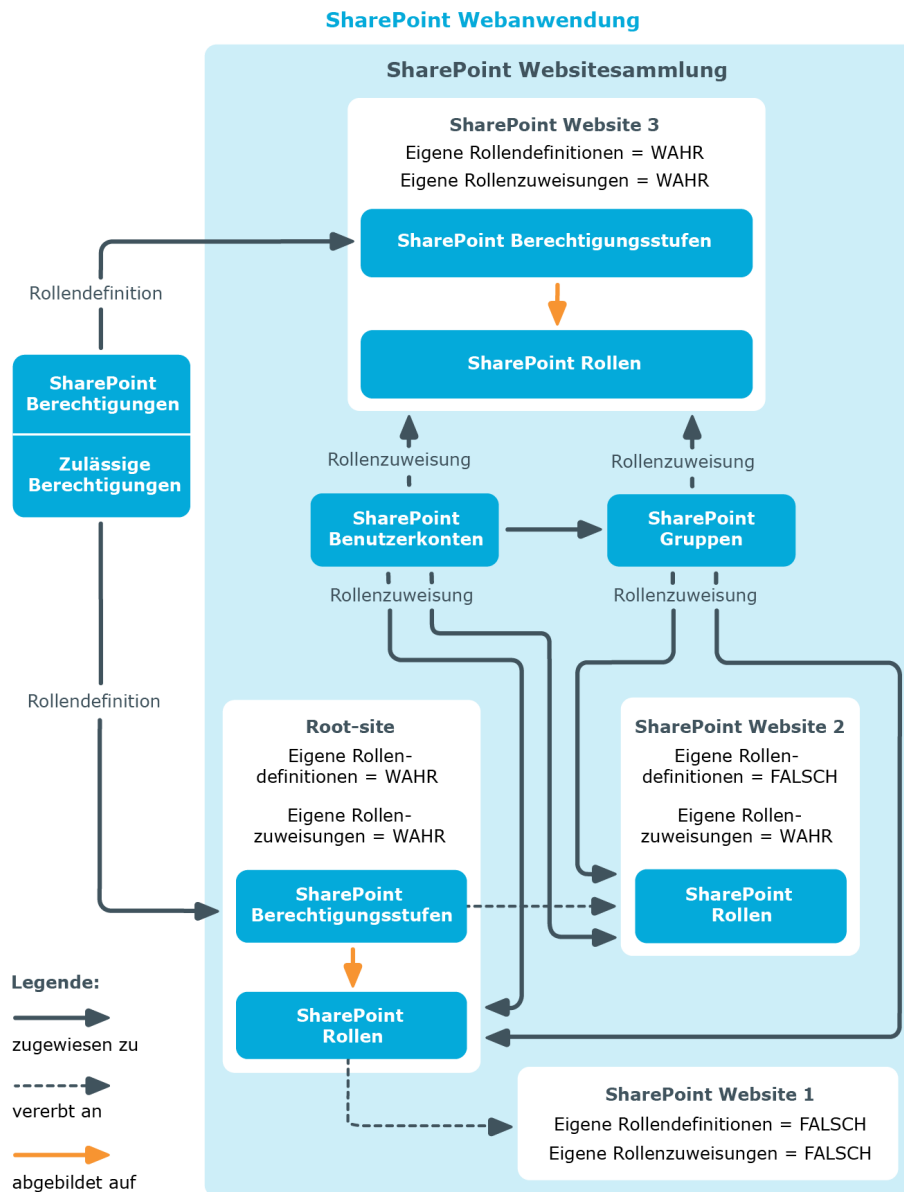
1. Die untergeordnete Website erbt die Rollendefinitionen und die Rollenzuweisungen.  
Es gelten sowohl die Berechtigungsstufen und Rollendefinitionen als auch die Rollenzuweisungen der übergeordneten (vererbenden) Website. Benutzerkonten und Gruppen können nicht explizit auf die Website berechtigt werden. Es haben nur die Benutzerkonten Zugriff auf diese Website, die auch auf die übergeordnete (vererbende) Website berechtigt sind.
2. Die untergeordnete Website erbt die Rollendefinitionen.  
An der untergeordneten Website können keine eigenen Berechtigungsstufen definiert werden. Die SharePoint Rollen dieser Website verweisen damit auf die Berechtigungsstufen der übergeordneten (vererbenden) Website und deren Rollendefinitionen. Benutzerkonten und Gruppen können an die darauf basierenden SharePoint Rollen der untergeordneten Website zugewiesen werden. Sind an der

untergeordneten Website eigene Berechtigungsstufen definiert, werden deren Berechtigungen durch die geerbten Berechtigungen überschrieben.

- Die untergeordnete Website erbt weder die Rollendefinitionen noch die Rollenzuweisungen.

Wie an der Root-Site einer Websitesammlung können hier eigene Berechtigungsstufen mit ihren Rollendefinitionen angelegt werden. Die darauf basierenden SharePoint Rollen werden an Benutzerkonten und Gruppen zugewiesen.

**Abbildung 2: Abbildung der Vererbung von SharePoint Berechtigungen an SharePoint Benutzerkonten im One Identity Manager**




# SharePoint Gruppen

Gruppen werden in SharePoint genutzt, um gleiche Berechtigungen an verschiedene Benutzer zu vergeben. Gruppen werden für eine Websitesammlung angelegt und sind für alle Websites dieser Websitesammlung gültig. Die für eine Website definierten SharePoint Rollen werden direkt an Gruppen zugewiesen. Alle Benutzerkonten, die Mitglied dieser Gruppen sind, erhalten die in den SharePoint Rollen definierten Berechtigungen auf diese Website.

Folgende Informationen über Gruppen können Sie im One Identity Manager bearbeiten:

- Objekteigenschaften wie Anzeigename, Eigentümer oder Sichtbarkeit von Mitgliedschaften
- Zugewiesene SharePoint Rollen und Benutzerkonten
- Nutzung im IT Shop
- Risikobewertung
- Vererbung über hierarchische Rollen und Einschränkung der Vererbung

## **Um die Stammdaten einer Gruppe zu bearbeiten**

1. Wählen Sie die Kategorie **SharePoint | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.  
- ODER -  
Klicken Sie in der Ergebnisliste .
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

## **Detaillierte Informationen zum Thema**

- [Erfassen der Stammdaten für SharePoint Gruppen](#) auf Seite 126

## **Verwandte Themen**

- [SharePoint Rollen und Gruppen](#) auf Seite 123

# Erfassen der Stammdaten für SharePoint Gruppen

**Tabelle 25: Konfigurationsparameter für die Einrichtung von SharePoint Gruppen**

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

Für eine Gruppe erfassen Sie die folgenden Stammdaten.

**Tabelle 26: Stammdaten einer SharePoint Gruppe**

Eigenschaft	Beschreibung
Anzeigename	Anzeigename der Gruppe.
Websitesammlung	Websitesammlung, in der die Gruppe angewendet wird.
Eigentümer	Eigentümer der Gruppe. Es kann entweder ein SharePoint Benutzerkonto oder eine SharePoint Gruppe ausgewählt werden.
Leistungsposition	Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
Alias der Verteilergruppe	Alias der Verteilergruppe, mit der die Gruppe verbunden ist.
E-Mail der Verteilergruppe	E-Mail-Adresse der Verteilergruppe, mit der die Gruppe verbunden ist.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Benutzerkonten. Stellen Sie einen Wert im Bereich von <b>0</b> bis <b>1</b> ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter <b>QER   CalculateRiskIndex</b> aktiviert ist.
Kategorie	Kategorien für die Vererbung von Gruppen. Gruppen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Beschreibung (HTML)	Zusätzliche Informationen über die Gruppe im HTML-Format.

Eigenschaft	Beschreibung
	(Wird im SharePoint im Beschreibungsfeld „Über mich“ angezeigt.)
Nur Gruppenmitglieder dürfen Mitgliedschaften sehen	Angabe, ob nur Mitglieder der Gruppe die Liste der Mitglieder sehen dürfen.
Gruppenmitglieder dürfen Mitgliedschaften bearbeiten	Angabe, ob alle Mitglieder der Gruppe die Mitgliedschaften der Gruppe bearbeiten dürfen.
Benutzer dürfen Mitgliedschaft beantragen	Angabe, ob SharePoint Benutzer die Mitgliedschaft in dieser Gruppe selbst beantragen oder beenden dürfen.
Auf Antrag automatische Mitgliedschaft	Angabe, ob SharePoint Benutzer automatisch Mitglied der Gruppe werden, sobald sie die Mitgliedschaft beantragen. Gleiches gilt, wenn Benutzer die Mitgliedschaft beenden.
E-Mail-Adresse Mitgliedschaftsantrag	E-Mail-Adresse, an die der Antrag auf Mitgliedschaft in der Gruppe beziehungsweise auf Beenden der Mitgliedschaft gesendet 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 bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.

## Detaillierte Informationen zum Thema

- [Festlegen der Kategorien für die Vererbung von SharePoint Gruppen](#) auf Seite 89
- [Vererbung von SharePoint Gruppen anhand von Kategorien](#) auf Seite 140
- One Identity Manager Administrationshandbuch für IT Shop
- One Identity Manager Administrationshandbuch für Risikobewertungen

# SharePoint Gruppen an SharePoint Benutzerkonten zuweisen

Gruppen können direkt oder indirekt an Identitäten zugewiesen werden. Bei der indirekten Zuweisung werden Identitäten und Gruppen in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der Gruppen, die einer Identität zugewiesen ist.

Wenn Sie eine Identität in hierarchische Rollen aufnehmen und die Identität ein benutzerauthentifiziertes Benutzerkonto besitzt, dann wird dieses Benutzerkonto in die Gruppe aufgenommen. Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Identitäten sind:

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Identitäten und Gruppen erlaubt.
- An den Benutzerkonten ist die Option **Gruppenauthentifiziert** deaktiviert.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.
- Benutzerkonten und Gruppen gehören zur selben Websitesammlung.

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

## Detaillierte Informationen zum Thema

- [SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 128
- [SharePoint Gruppen an Geschäftsrollen zuweisen](#) auf Seite 130
- [SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen](#) auf Seite 131
- [SharePoint Rollen an SharePoint Gruppen zuweisen](#) auf Seite 132
- [SharePoint Gruppen in Systemrollen aufnehmen](#) auf Seite 132
- [SharePoint Gruppen in den IT Shop aufnehmen](#) auf Seite 133
- [SharePoint Gruppen automatisch in den IT Shop aufnehmen](#) auf Seite 135
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

## SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Gruppe an Abteilungen, Kostenstellen oder Standorte zu, damit sie über diese Organisationen an Benutzerkonten zugewiesen wird.




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

1. Wählen Sie im Manager die Kategorie **SharePoint > 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 **SharePoint 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**

- [SharePoint Gruppen an Geschäftsrollen zuweisen](#) auf Seite 130
- [SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen](#) auf Seite 131
- [SharePoint Rollen an SharePoint Gruppen zuweisen](#) auf Seite 132
- [SharePoint Gruppen in Systemrollen aufnehmen](#) auf Seite 132

- [SharePoint Gruppen in den IT Shop aufnehmen](#) auf Seite 133
- [SharePoint Gruppen automatisch in den IT Shop aufnehmen](#) auf Seite 135
- [One Identity Manager Benutzer für die Verwaltung einer SharePoint-Umgebung](#) auf Seite 10

## SharePoint Gruppen an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul


Weisen Sie Gruppen an Geschäftsrollen zu, damit sie über diese Geschäftsrollen an Benutzerkonten zugewiesen werden.

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

1. Wählen Sie im Manager die Kategorie **SharePoint > 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 **SharePoint 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

- [SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 128
- [SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen](#) auf Seite 131
- [SharePoint Rollen an SharePoint Gruppen zuweisen](#) auf Seite 132
- [SharePoint Gruppen in Systemrollen aufnehmen](#) auf Seite 132
- [SharePoint Gruppen in den IT Shop aufnehmen](#) auf Seite 133
- [SharePoint Gruppen automatisch in den IT Shop aufnehmen](#) auf Seite 135
- [One Identity Manager Benutzer für die Verwaltung einer SharePoint-Umgebung](#) auf Seite 10

# SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen

Gruppen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Die indirekte Zuweisung kann nur für benutzerauthentifizierte Benutzerkonten genutzt werden. Die direkte Zuweisung kann für gruppen- und benutzerauthentifizierte Benutzerkonten genutzt werden.

Benutzerkonten und Gruppen müssen zur selben Websitesammlung gehören.

### ***Um eine Gruppe direkt an Benutzerkonten zuzuweisen***

1. Wählen Sie die Kategorie **SharePoint | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.  
- ODER -  
Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
5. Speichern Sie die Änderungen.

## Verwandte Themen

- [SharePoint Gruppen direkt an ein SharePoint Benutzerkonto zuweisen](#) auf Seite 113
- [SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 128
- [SharePoint Gruppen an Geschäftsrollen zuweisen](#) auf Seite 130
- [SharePoint Rollen an SharePoint Gruppen zuweisen](#) auf Seite 132
- [SharePoint Gruppen in Systemrollen aufnehmen](#) auf Seite 132

- [SharePoint Gruppen in den IT Shop aufnehmen](#) auf Seite 133
- [SharePoint Gruppen automatisch in den IT Shop aufnehmen](#) auf Seite 135

## SharePoint Rollen an SharePoint Gruppen zuweisen

Damit SharePoint Benutzerkonten Berechtigungen auf die einzelnen Websites erhalten, weisen Sie den Gruppen SharePoint Rollen zu. SharePoint Rollen und Gruppen müssen zur selben Websitesammlung gehören.

**HINWEIS:** SharePoint Rollen, die auf Berechtigungsstufen verweisen, bei denen die Option **Versteckt** aktiviert ist, können nicht an Gruppen zugewiesen werden.

### Um SharePoint Rollen an eine Gruppe zuzuweisen

1. Wählen Sie die Kategorie **SharePoint | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **SharePoint Rollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Rollen zu.
  - ODER -
  - Entfernen Sie im Bereich **Zuordnungen entfernen** die Rollen.
5. Speichern Sie die Änderungen.

### Verwandte Themen

- [Erfassen der Stammdaten für SharePoint Berechtigungsstufen](#) auf Seite 145
- [SharePoint Gruppen an SharePoint Rollen zuweisen](#) auf Seite 153
- [SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 128
- [SharePoint Gruppen an Geschäftsrollen zuweisen](#) auf Seite 130
- [SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen](#) auf Seite 131
- [SharePoint Gruppen in Systemrollen aufnehmen](#) auf Seite 132
- [SharePoint Gruppen in den IT Shop aufnehmen](#) auf Seite 133
- [SharePoint Gruppen automatisch in den IT Shop aufnehmen](#) auf Seite 135

## SharePoint 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 Identitäten zuweisen, wird die Gruppe an alle benutzerauthentifizierten Benutzerkonten vererbt, die diese Identitäten besitzen.


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

### Um eine Gruppe an Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **SharePoint > 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

- [SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 128
- [SharePoint Gruppen an Geschäftsrollen zuweisen](#) auf Seite 130
- [SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen](#) auf Seite 131
- [SharePoint Rollen an SharePoint Gruppen zuweisen](#) auf Seite 132
- [SharePoint Gruppen in den IT Shop aufnehmen](#) auf Seite 133
- [SharePoint Gruppen automatisch in den IT Shop aufnehmen](#) auf Seite 135

## SharePoint 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 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 Identitäten 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 **SharePoint > Gruppen** (bei nicht-rollenbasierter Anmeldung).  
- ODER -  
Wählen Sie im Manager die Kategorie **Berechtigungen > SharePoint 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 **SharePoint > Gruppen** (bei nicht-rollenbasierter Anmeldung).  
- ODER -  
Wählen Sie im Manager die Kategorie **Berechtigungen > SharePoint 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 **SharePoint > Gruppen** (bei nicht-rollenbasierter Anmeldung).  
- ODER -  
Wählen Sie im Manager die Kategorie **Berechtigungen > SharePoint 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

- [Erfassen der Stammdaten für SharePoint Gruppen](#) auf Seite 126
- [SharePoint Gruppen automatisch in den IT Shop aufnehmen](#) auf Seite 135
- [SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 128
- [SharePoint Gruppen an Geschäftsrollen zuweisen](#) auf Seite 130
- [SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen](#) auf Seite 131
- [SharePoint Rollen an SharePoint Gruppen zuweisen](#) auf Seite 132
- [SharePoint Gruppen in Systemrollen aufnehmen](#) auf Seite 132

## SharePoint Gruppen automatisch in den IT Shop aufnehmen

Mit den folgenden Schritten können SharePoint Gruppen automatisch in den IT Shop aufgenommen werden. Die Synchronisation sorgt dafür, dass die SharePoint Gruppen in den IT Shop aufgenommen werden. Bei Bedarf können Sie die Synchronisation im Synchronization Editor sofort starten. SharePoint Gruppen, die im One Identity Manager neu erstellt werden, werden ebenfalls automatisch in den IT Shop aufgenommen.

### Um SharePoint Gruppen automatisch in den IT Shop aufzunehmen

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | SPSGroup**.
2. Um einzelne SharePoint Gruppen nicht automatisch in den IT Shop aufzunehmen, aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | SPSGroup | ExcludeList**.

Der Konfigurationsparameter enthält eine Auflistung aller SharePoint Gruppen, die nicht automatisch zum IT Shop zugeordnet werden sollen. Bei Bedarf können Sie die Liste erweitern. Erfassen Sie dazu im Wert des Konfigurationsparameters die Namen der Gruppen. Die Namen werden in einer Pipe (|) getrennten Liste angegeben. Reguläre Ausdrücke werden unterstützt.

3. Kompilieren Sie die Datenbank.

Die SharePoint Gruppen werden ab diesem Zeitpunkt automatisch in den IT Shop aufgenommen.

Folgende Schritte werden bei der Aufnahme einer SharePoint Gruppe in den IT Shop automatisch ausgeführt.

1. Es wird eine Leistungsposition für die SharePoint Gruppe ermittelt.

Für jede SharePoint Gruppe wird die Leistungsposition geprüft und bei Bedarf angepasst. Die Bezeichnung der Leistungsposition entspricht der Bezeichnung der SharePoint Gruppe.

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

2. Die Leistungsposition wird der Standard-Servicekategorie **SharePoint Gruppen** zugeordnet.

3. Es wird eine Anwendungsrolle für Produkteigner ermittelt und der Leistungsposition zugeordnet.

Die Produkteigner können Bestellungen von Mitgliedschaften in diesen SharePoint Gruppen genehmigen. Standardmäßig wird der Eigentümer einer SharePoint Gruppe als Produkteigner ermittelt.

**HINWEIS:** Die Anwendungsrolle für Produkteigner muss der Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner** untergeordnet sein.

- Ist der Eigentümer der SharePoint Gruppe bereits Mitglied einer Anwendungsrolle für Produkteigner, dann wird diese Anwendungsrolle der Leistungsposition zugewiesen. Alle Mitglieder dieser Anwendungsrolle werden dadurch Produkteigner der SharePoint Gruppe.
- Ist der Eigentümer der SharePoint Gruppe noch kein Mitglied einer Anwendungsrolle für Produkteigner, dann wird eine neue Anwendungsrolle erzeugt. Die Bezeichnung der Anwendungsrolle entspricht der Bezeichnung des Eigentümers.
  - Handelt es sich beim Eigentümer um ein Benutzerkonto, wird die Identität des Benutzerkontos in die Anwendungsrolle aufgenommen.
  - Handelt es sich um eine Gruppe von Eigentümern, werden die Identitäten aller Benutzerkonten dieser Gruppe in die Anwendungsrolle aufgenommen.
- Besitzt die SharePoint Gruppe keine Eigentümer wird die Standard-Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner | Ohne Eigentümer im SharePoint** verwendet.

4. Die SharePoint Gruppe wird mit der Option **IT Shop** gekennzeichnet und dem IT Shop Regal **SharePoint Gruppen** im Shop **Identity & Access Lifecycle** zugewiesen.

Anschließend können die Kunden des Shops Mitgliedschaften in SharePoint Gruppen über das Web Portal bestellen.



**HINWEIS:** Wenn eine SharePoint Gruppe endgültig aus der One Identity Manager-Datenbank gelöscht wird, wird auch die zugehörige Leistungsposition gelöscht.

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

## Verwandte Themen

- [SharePoint Gruppen in den IT Shop aufnehmen](#) auf Seite 133
- [SharePoint Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 128
- [SharePoint Gruppen an Geschäftsrollen zuweisen](#) auf Seite 130
- [SharePoint Benutzerkonten direkt an eine SharePoint Gruppe zuweisen](#) auf Seite 131
- [SharePoint Rollen an SharePoint Gruppen zuweisen](#) auf Seite 132
- [SharePoint Gruppen in Systemrollen aufnehmen](#) auf Seite 132
- [Standardlösungen für die Bestellung von SharePoint Gruppen](#) auf Seite 143

## Zusätzliche Aufgaben für die Verwaltung von SharePoint Gruppen

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

### Überblick über die SharePoint Gruppe

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

## Wirksamkeit von Gruppenmitgliedschaften

Bei der Zuweisung von Gruppen an Benutzerkonten kann es vorkommen, dass eine Identität zwei oder mehr Gruppen erhält, die in dieser Kombination nicht auftreten dürfen.

Um das zu verhindern, geben Sie die sich ausschließenden Gruppen bekannt. Dabei legen Sie für zwei Gruppen fest, welche der beiden Gruppen an Benutzerkonten wirksam werden soll, wenn beide zugewiesen sind.

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

#### HINWEIS:

- Ein wechselseitiger Ausschluss zweier Gruppen kann nicht definiert werden. Das heißt, die Festlegung "Gruppe A schließt Gruppe B aus" UND "Gruppe B schließt Gruppe A aus" ist nicht zulässig.
- Für eine Gruppe muss jede auszuschließende Gruppe einzeln bekannt gegeben werden. Ausschlussdefinitionen werden nicht vererbt.

Die Wirksamkeit der Zuweisungen wird in den Tabellen SPUserInSPSGroup und BaseTreeHasSPSGroup über die Spalte XIsInEffect abgebildet.

### Beispiel: Wirksamkeit von Gruppenmitgliedschaften

- In einer Websitesammlung 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 Websitesammlung. 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 Identität 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 27: Festlegen der ausgeschlossenen Gruppen (Tabelle SPGroupExclusion)**

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

**Tabelle 28: Wirksame Zuweisungen**

Identität	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 29: Ausgeschlossene Gruppen und wirksame Zuweisungen**

Identität	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 | Inherit | 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 Websitesammlung.

## Um Gruppen auszuschließen

- Wählen Sie im Manager die Kategorie **SharePoint > Gruppen**.
- 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 SharePoint 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**.

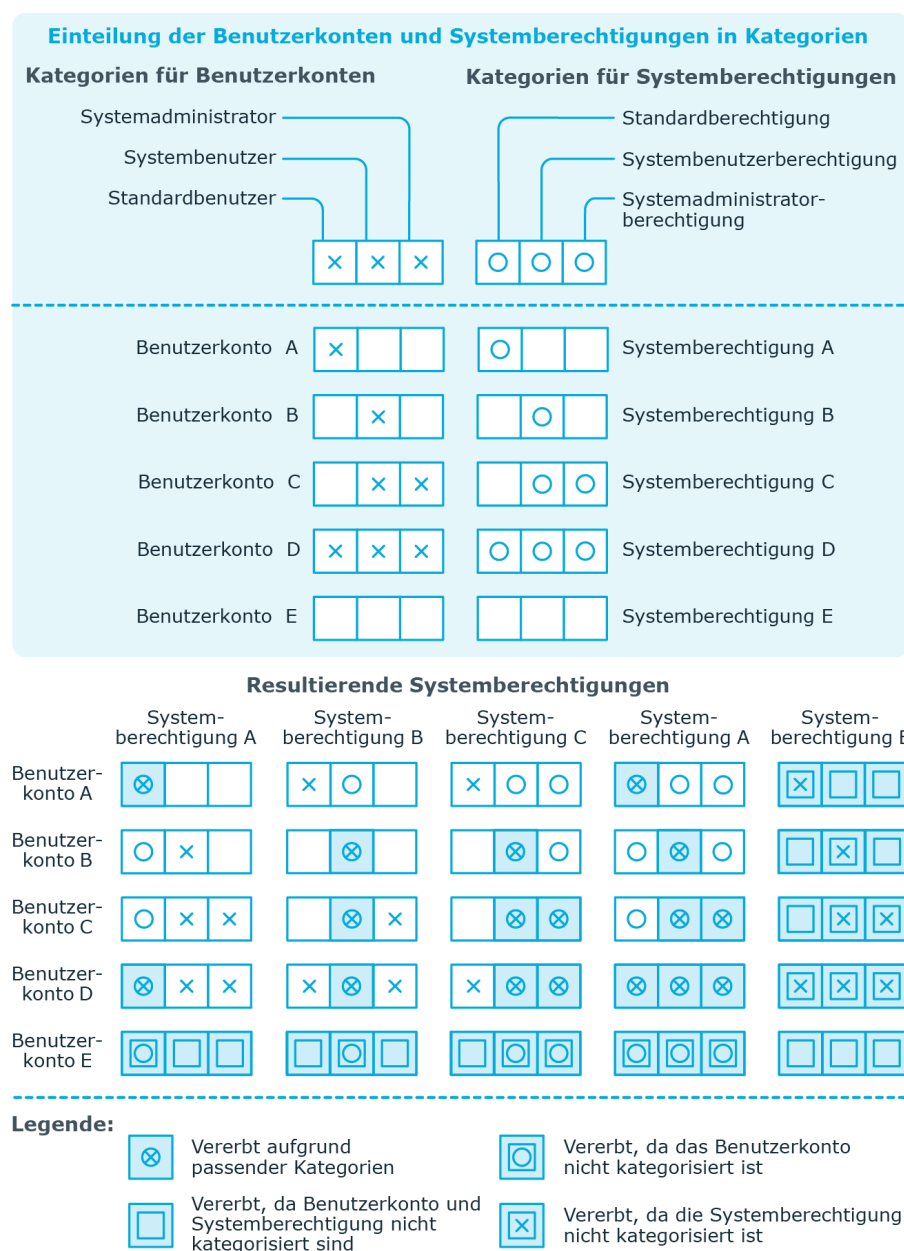
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto vererbt. Ist 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 30: Beispiele für Kategorien**

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

**Abbildung 3: Beispiel für die Vererbung über Kategorien**



### Um die Vererbung über Kategorien zu nutzen

1. Definieren Sie an der Websitesammlung 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

- [Festlegen der Kategorien für die Vererbung von SharePoint Gruppen](#) auf Seite 89
- [Stammdaten eines benutzerauthentifizierten Benutzerkontos](#) auf Seite 107
- [Stammdaten eines gruppenauthentifizierten Benutzerkontos](#) auf Seite 103
- [Erfassen der Stammdaten für SharePoint Gruppen](#) auf Seite 126

## Zusatzeigenschaften an SharePoint 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 **SharePoint > 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.

## Löschen von SharePoint Gruppen

### Um eine Gruppe zu löschen

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

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

# Standardlösungen für die Bestellung von SharePoint Gruppen

Im One Identity Manager werden Standardprodukte und Standard-Entscheidungsworkflows bereitgestellt, um SharePoint Gruppen sowie Mitgliedschaften in diesen Gruppen über den IT Shop zu bestellen. Dadurch werden Berechtigungen in den Zielsystemen über definierte Genehmigungsverfahren vergeben.

Ausführliche Informationen dazu finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.

## Detaillierte Informationen zum Thema

- [Anlegen von SharePoint Gruppen](#) auf Seite 143
- [SharePoint Gruppenmitgliedschaften bestellen](#) auf Seite 144

## Anlegen von SharePoint Gruppen

Über die Bestellung dieses Standardprodukts können neue SharePoint Gruppen in der SharePoint-Umgebung angelegt werden. Der Besteller gibt Informationen über Namen und Websitesammlung, soweit bekannt, der Bestellung mit. Anhand dieser Informationen bestimmt der Zielsystemverantwortliche die Websitesammlung, in der die Gruppe angelegt werden soll, und genehmigt die Bestellung. Die Gruppe wird im One Identity Manager angelegt und in das Zielsystem publiziert.

### Voraussetzung

- Der Anwendungsrolle **Zielsysteme | SharePoint** sind Identitäten zugewiesen.

Wenn der Konfigurationsparameter **QER | ITShop | AutoPublish | SPSGroup** aktiviert ist, wird die Gruppe in den IT Shop aufgenommen und dem Regal **Identity & Access Lifecycle | SharePoint Gruppen** zugewiesen. Die Gruppe wird einer vorhandenen Servicekategorie zugeordnet.

**Tabelle 31: Standardprodukt für die Bestellung einer SharePoint Gruppe**

Produkt:	Anlegen einer SharePoint Gruppe
Servicekategorie:	SharePoint Gruppen
Regal:	Identity & Access Lifecycle   Gruppen Lifecycle
Entscheidungsrichtlinie/ Entscheidungsworkflow:	Entscheidung der Bestellungen zur Neuanlage von SharePoint Gruppen

## Verwandte Themen

- [SharePoint Gruppen automatisch in den IT Shop aufnehmen](#) auf Seite 135

# SharePoint Gruppenmitgliedschaften bestellen

Produkteigner und Zielsystemverantwortliche können im Web Portal Mitgliedschaften für die Gruppen in diesen Regalen bestellen. Der jeweilige Produkteigner oder Zielsystemverantwortliche muss diese Änderung genehmigen. Die Änderung wird in das Zielsystem publiziert.

**Tabelle 32: Standardobjekte für das Bestellen von Gruppenmitgliedschaften**

Regale:	Identity & Access Lifecycle   SharePoint Gruppen
Entscheidungsrichtlinien/ Entscheidungsworkflows:	Entscheidung der Bestellungen von Gruppenmitgliedschaften

## Verwandte Themen

- [SharePoint Gruppen automatisch in den IT Shop aufnehmen](#) auf Seite 135
- [Anlegen von SharePoint Gruppen](#) auf Seite 143

# SharePoint Rollen und Berechtigungsstufen

Um Berechtigungen auf die Objekte einer Website zu vergeben, werden in SharePoint sogenannte Berechtigungsstufen definiert. Diese Berechtigungsstufen fassen verschiedene SharePoint Berechtigungen zusammen. Berechtigungsstufen, die einen eindeutigen Bezug zu einer Website haben, werden in der One Identity Manager-Datenbank als SharePoint Rollen abgebildet. SharePoint Rollen können über Gruppen oder direkt an Benutzerkonten zugewiesen werden. Darüber erhalten die SharePoint Benutzer ihre Berechtigungen auf die Objekte einer Website.



[illegible]

### Um die Stammdaten einer Berechtigungsstufe zu bearbeiten

- Für eine Berechtigungsstufe erfassen Sie die folgenden Stammdaten.

**Tabelle 33: Eigenschaften einer Berechtigungsstufe**

Eigenschaft	Beschreibung
Berechtigungsstufe	Bezeichnung der Berechtigungsstufe.
Website	Eindeutige Kennung der Website, in der die Berechtigungsstufe angelegt ist.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Versteckt	Angabe, ob eine SharePoint Rolle mit dieser Berechtigungsstufe an Benutzerkonten oder Gruppen zugewiesen werden kann.

## Zusätzliche Aufgaben für die Verwaltung von SharePoint Berechtigungsstufen

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

### Überblick über die SharePoint Berechtigungsstufe

#### *Um einen Überblick über eine Berechtigungsstufe zu erhalten*

1. Wählen Sie die Kategorie **SharePoint | Berechtigungsstufen**.
2. Wählen Sie in der Ergebnisliste die Berechtigungsstufe.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Berechtigungsstufe**.

### Berechtigungen zuweisen

Im One Identity Manager können Sie SharePoint Berechtigungen an Berechtigungsstufen zuweisen. Dabei können nur die für die Webanwendung zulässigen Berechtigungen zugewiesen werden. Über die SharePoint-internen Vererbungsvorgänge erhalten Benutzerkonten diese Berechtigungen auf eine Website.

Berechtigungen können von anderen Berechtigungen abhängig sein. SharePoint weist diese abhängigen Berechtigungen automatisch zu. Beispielsweise werden mit der Berechtigung "Create Groups" immer auch die Berechtigungen "View Pages", "Browse User Information" und "Open" vergeben werden.

**HINWEIS:** Abhängige Berechtigungen können im One Identity Manager nicht automatisch an Berechtigungsstufen zugewiesen werden.

### Um Berechtigungen an Berechtigungsstufen zuzuweisen

1. Wählen Sie die Kategorie **SharePoint | Berechtigungsstufen**.
2. Wählen Sie in der Ergebnisliste die Berechtigungsstufe.
3. Wählen Sie die Aufgabe **Berechtigungen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungen zu.  
- ODER -  
Entfernen Sie im Bereich **Zuordnungen entfernen** die Berechtigungen.
5. Speichern Sie die Änderungen.

### Verwandte Themen

- [SharePoint Rollen und Gruppen](#) auf Seite 123

## Besonderheiten bei der Synchronisation zulässiger Berechtigungen

Wenn in der SharePoint-Umgebung eine Berechtigung aus der Liste der zulässigen Berechtigungen für eine Webanwendung entfernt wird, kann diese Berechtigung ab diesem Zeitpunkt keiner Berechtigungsstufe innerhalb der Webanwendung zugewiesen werden. Bereits bestehende Zuweisungen der Berechtigung zu einer Berechtigungsstufe bleiben erhalten, sind jedoch nicht wirksam. Bei der Synchronisation wird diese Berechtigung aus der Tabelle SPSWebAppHasPermission gelöscht. Bereits bestehende Zuweisungen der Berechtigung zu einer Berechtigungsstufe werden nicht geändert. Die unwirksamen Berechtigungen werden auf dem Übersichtformular der Berechtigungsstufen angezeigt.

## Erfassen der Stammdaten für SharePoint Rollen

**Tabelle 34: Konfigurationsparameter für die Einrichtung von SharePoint Rollen**

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

### Um die Stammdaten einer SharePoint Rolle zu bearbeiten

1. Wählen Sie die Kategorie **SharePoint | Rollen**.
2. Wählen Sie in der Ergebnisliste die SharePoint Rolle. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Für SharePoint Rollen werden die folgenden Stammdaten abgebildet.

**Tabelle 35: Eigenschaften einer SharePoint Rolle**

Eigenschaft	Beschreibung
Anzeigename	Anzeigename der SharePoint Rolle.
Berechtigungsstufe	Eindeutige Kennung der Berechtigungsstufe, aus der die SharePoint Rolle gebildet ist.
Website	Eindeutige Kennung der Website, an die die SharePoint Rolle ihre Berechtigungen vererbt.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der SharePoint Rolle an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter "QER\CalculateRiskIndex" aktiviert ist.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Leistungsposition	Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
IT Shop	Angabe, ob die SharePoint Rolle über den IT Shop bestellbar ist. Die SharePoint Rolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die SharePoint Rolle kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die SharePoint Rolle ausschließlich über den IT Shop bestellbar ist. Die SharePoint Rolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der SharePoint Rolle an hierarchische Rollen ist nicht zulässig.

**HINWEIS:** Wenn die SharePoint Rolle auf eine Berechtigungsstufe verweist, bei der die Option **Versteckt** aktiviert ist, können die Optionen **IT Shop** und **Verwendung nur im IT Shop** nicht aktiviert werden. Diese SharePoint Rollen können nicht an Benutzerkonten oder Gruppen zugewiesen werden.

## Detaillierte Informationen zum Thema

- [Erfassen der Stammdaten für SharePoint Berechtigungsstufen](#) auf Seite 145
- One Identity Manager Administrationshandbuch für IT Shop
- One Identity Manager Administrationshandbuch für Risikobewertungen

# SharePoint Rollen an SharePoint Benutzerkonten zuweisen

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

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Identitäten und Gruppen erlaubt.
- An den Benutzerkonten ist die Option **Gruppenauthentifiziert** deaktiviert.
- Die Benutzerkonten sind mit der Option **Rollen erbbar** gekennzeichnet.
- Benutzerkonten und SharePoint Rollen gehören zur selben Websitesammlung.

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

**HINWEIS:** Wenn die SharePoint Rolle auf eine Berechtigungsstufe verweist, bei der die Option **Versteckt** aktiviert ist, können keine Geschäftsrollen und Organisationen zugewiesen werden. Diese SharePoint Rollen können weder direkt noch indirekt an Benutzerkonten oder Gruppen zugewiesen werden.

## Detaillierte Informationen zum Thema

- [Erfassen der Stammdaten für SharePoint Berechtigungsstufen](#) auf Seite 145
- [SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 150
- [SharePoint Rollen an Geschäftsrollen zuweisen](#) auf Seite 151
- [SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen](#) auf Seite 152
- [SharePoint Gruppen an SharePoint Rollen zuweisen](#) auf Seite 153

- [SharePoint Rollen in Systemrollen aufnehmen](#) auf Seite 153
- [SharePoint Rollen in den IT Shop aufnehmen](#) auf Seite 154
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

## SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen


Weisen Sie die SharePoint Rolle an Abteilungen, Kostenstellen oder Standorte zu, damit sie über diese Organisationen an Benutzerkonten zugewiesen wird.

### ***Um eine SharePoint Rolle an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **SharePoint | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
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 SharePoint Rollen an eine Abteilung, eine Kostenstellen oder einen Standorte zuzuweisen (bei rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **Organisationen | Abteilungen**.
  - ODER -
  - Wählen Sie die Kategorie **Organisationen | Kostenstellen**.
  - ODER -
  - Wählen Sie die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **SharePoint Rollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die SharePoint Rollen zu.
  - ODER -

- Entfernen Sie im Bereich **Zuordnungen entfernen** die SharePoint Rollen.
5. Speichern Sie die Änderungen.

## Verwandte Themen

- [SharePoint Rollen an Geschäftsrollen zuweisen](#) auf Seite 151
- [SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen](#) auf Seite 152
- [SharePoint Gruppen an SharePoint Rollen zuweisen](#) auf Seite 153
- [SharePoint Rollen in Systemrollen aufnehmen](#) auf Seite 153
- [SharePoint Rollen in den IT Shop aufnehmen](#) auf Seite 154
- [One Identity Manager Benutzer für die Verwaltung einer SharePoint-Umgebung](#) auf Seite 10

# SharePoint Rollen an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie SharePoint Rollen an Geschäftsrollen zu, damit sie über diese Geschäftsrollen an Benutzerkonten zugewiesen werden.

### ***Um eine SharePoint Rolle an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **SharePoint | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.
  - ODER -Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
5. Speichern Sie die Änderungen.

### ***Um SharePoint Rollen an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **SharePoint Rollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die SharePoint Rollen zu.
  - ODER -Entfernen Sie im Bereich **Zuordnungen entfernen** die SharePoint Rollen.
5. Speichern Sie die Änderungen.

## Verwandte Themen

- [SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 150
- [SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen](#) auf Seite 152
- [SharePoint Gruppen an SharePoint Rollen zuweisen](#) auf Seite 153
- [SharePoint Rollen in Systemrollen aufnehmen](#) auf Seite 153
- [SharePoint Rollen in den IT Shop aufnehmen](#) auf Seite 154
- [One Identity Manager Benutzer für die Verwaltung einer SharePoint-Umgebung](#) auf Seite 10

# SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen

SharePoint Rollen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Die indirekte Zuweisung kann nur für benutzerauthentifizierte Benutzerkonten genutzt werden. Die direkte Zuweisung kann für gruppen- und benutzerauthentifizierte Benutzerkonten genutzt werden.

Benutzerkonten und SharePoint Rollen müssen zur selben Websitesammlung gehören.

**HINWEIS:** Wenn die SharePoint Rolle auf eine Berechtigungsstufe verweist, bei der die Option **Versteckt** aktiviert ist, können keine Benutzerkonten zugewiesen werden.

### **Um eine SharePoint Rolle direkt an Benutzerkonten zuzuweisen**

1. Wählen Sie die Kategorie **SharePoint | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.  
- ODER -  
Entfernen Sie im Bereich **Zuordnungen entfernen** die Benutzerkonten.
5. Speichern Sie die Änderungen.

## Verwandte Themen

- [Erfassen der Stammdaten für SharePoint Berechtigungsstufen](#) auf Seite 145
- [SharePoint Rollen direkt an ein Benutzerkonto zuweisen](#) auf Seite 114
- [SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 150
- [SharePoint Rollen an Geschäftsrollen zuweisen](#) auf Seite 151
- [SharePoint Gruppen an SharePoint Rollen zuweisen](#) auf Seite 153



- [SharePoint Rollen in Systemrollen aufnehmen](#) auf Seite 153
- [SharePoint Rollen in den IT Shop aufnehmen](#) auf Seite 154

## SharePoint Gruppen an SharePoint Rollen zuweisen

Damit SharePoint Benutzerkonten Berechtigungen auf die einzelnen Websites erhalten, weisen Sie den Gruppen SharePoint Rollen zu. SharePoint Rollen und Gruppen müssen zur selben Websitesammlung gehören.

**HINWEIS:** SharePoint Rollen, die auf Berechtigungsstufen verweisen, bei denen die Option **Versteckt** aktiviert ist, können nicht an Gruppen zugewiesen werden.

### Um Gruppen an eine SharePoint Rolle zuzuweisen

1. Wählen Sie die Kategorie **SharePoint | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.  
- ODER -  
Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
5. Speichern Sie die Änderungen.

### Verwandte Themen

- [Erfassen der Stammdaten für SharePoint Berechtigungsstufen](#) auf Seite 145
- [SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 150
- [SharePoint Rollen an Geschäftsrollen zuweisen](#) auf Seite 151
- [SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen](#) auf Seite 152
- [SharePoint Rollen an SharePoint Gruppen zuweisen](#) auf Seite 132
- [SharePoint Rollen in Systemrollen aufnehmen](#) auf Seite 153
- [SharePoint Rollen in den IT Shop aufnehmen](#) auf Seite 154

## SharePoint Rollen in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

Mit dieser Aufgabe nehmen Sie eine SharePoint Rolle in Systemrollen auf. Wenn Sie eine Systemrolle an Identitäten zuweisen, wird die SharePoint Rolle an alle benutzerauthentifizierten Benutzerkonten vererbt, die diese Identitäten besitzen.

**HINWEIS:** Wenn die SharePoint Rolle auf eine Berechtigungsstufe verweist, bei der die Option **Versteckt** aktiviert ist, können keine Systemrollen zugewiesen werden. Diese SharePoint Rollen können weder direkt noch indirekt an Benutzerkonten oder Gruppen zugewiesen werden. Weitere Informationen finden Sie unter [Erfassen der Stammdaten für SharePoint Berechtigungsstufen](#) auf Seite 145.


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

### **Um eine SharePoint Rolle an Systemrollen zuzuweisen**

1. Wählen Sie die Kategorie **SharePoint | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
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**

- [SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 150
- [SharePoint Rollen an Geschäftsrollen zuweisen](#) auf Seite 151
- [SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen](#) auf Seite 152
- [SharePoint Rollen an SharePoint Gruppen zuweisen](#) auf Seite 132
- [SharePoint Rollen in den IT Shop aufnehmen](#) auf Seite 154

## **SharePoint Rollen in den IT Shop aufnehmen**

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

- Die SharePoint Rolle muss mit der Option **IT Shop** gekennzeichnet sein.
- Der SharePoint Rolle muss eine Leistungsposition zugeordnet sein.
- Soll die SharePoint Rolle nur über IT Shop-Bestellungen an Identitäten zugewiesen werden können, muss die SharePoint Rolle 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 Administratoren für den IT Shop SharePoint Rollen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt SharePoint Rollen in den IT Shop aufzunehmen.

### ***Um eine SharePoint Rolle in den IT Shop aufzunehmen***

1. Wählen Sie die Kategorie **SharePoint | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

### ***Um eine SharePoint Rolle aus einzelnen Regalen des IT Shops zu entfernen***

1. Wählen Sie die Kategorie **SharePoint | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppe aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

### ***Um eine SharePoint Rolle aus allen Regalen des IT Shops zu entfernen***

1. Wählen Sie die Kategorie **SharePoint | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

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

## **Detaillierte Informationen zum Thema**

- One Identity Manager Administrationshandbuch für IT Shop

## **Verwandte Themen**

- [Erfassen der Stammdaten für SharePoint Rollen](#) auf Seite 147
- [SharePoint Rollen an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 150
- [SharePoint Rollen an Geschäftsrollen zuweisen](#) auf Seite 151
- [SharePoint Benutzerkonten direkt an eine SharePoint Rolle zuweisen](#) auf Seite 152

- [SharePoint Gruppen an SharePoint Rollen zuweisen](#) auf Seite 153
- [SharePoint Rollen in Systemrollen aufnehmen](#) auf Seite 153

## Zusätzliche Aufgaben für die Verwaltung von SharePoint Rollen

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

### Überblick über die SharePoint Rolle

*Um einen Überblick über eine SharePoint Rolle zu erhalten*

1. Wählen Sie die Kategorie **SharePoint | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Rolle**.

### Wirksamkeit von SharePoint Rollen

Das unter [Wirksamkeit von Gruppenmitgliedschaften](#) auf Seite 137 beschriebene Verhalten können Sie auch für SharePoint Rollen nutzen.

Die Wirksamkeit der Zuweisungen wird in den Tabellen SPSUserHasSPSRLAssign und BaseTreeHasSPSRLAssign über die Spalte XIsInEffect abgebildet.

### Voraussetzungen

- Der Konfigurationsparameter **QER | Structures | Inherit | 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 SharePoint Rollen gehören zur selben Websitesammlung.

### **Um SharePoint Rollen auszuschließen**

1. Wählen Sie die Kategorie **SharePoint | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **SharePoint Rollen ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Rollen zu, die sich mit der gewählten Rolle ausschließen.
  - ODER -Entfernen Sie im Bereich **Zuordnungen entfernen** die Rollen, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

### **Detaillierte Informationen zum Thema**

- [Wirksamkeit von Gruppenmitgliedschaften](#) auf Seite 137

## **Zusatzeigenschaften an SharePoint Rollen zuweisen**


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

### **Um Zusatzeigenschaften für eine SharePoint Rolle festzulegen**

1. Wählen Sie im Manager die Kategorie **SharePoint | Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

#### **Um eine Zuweisung zu entfernen**


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

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

# Löschen von SharePoint Rollen und Berechtigungsstufen


SharePoint Rollen können im Manager nicht gelöscht werden. Sie werden durch den DBQueue Prozessor gelöscht, wenn die zugehörige Berechtigungsstufe gelöscht wird.

## **Um eine Berechtigungsstufe zu löschen**

1. Wählen Sie die Kategorie **SharePoint | Berechtigungsstufen**.
2. Wählen Sie in der Ergebnisliste die Berechtigungsstufe.
3. Klicken Sie , um die Berechtigungsstufe zu löschen.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Wenn eine Löschverzögerung konfiguriert ist, wird die Berechtigungsstufe zum Löschen markiert und erst nach Ablauf der Löschverzögerung endgültig gelöscht. Während dieser Zeit kann die Berechtigungsstufe wiederhergestellt werden. Berechtigungsstufen mit einer Löschverzögerung von 0 Tagen werden sofort gelöscht.

## **Um eine Berechtigungsstufe wiederherzustellen**

1. Wählen Sie die Kategorie **SharePoint | Berechtigungsstufen**.
2. Wählen Sie in der Ergebnisliste die zum Löschen markierte Berechtigungsstufe.
3. Klicken Sie in der Ergebnisliste .

## **Verwandte Themen**

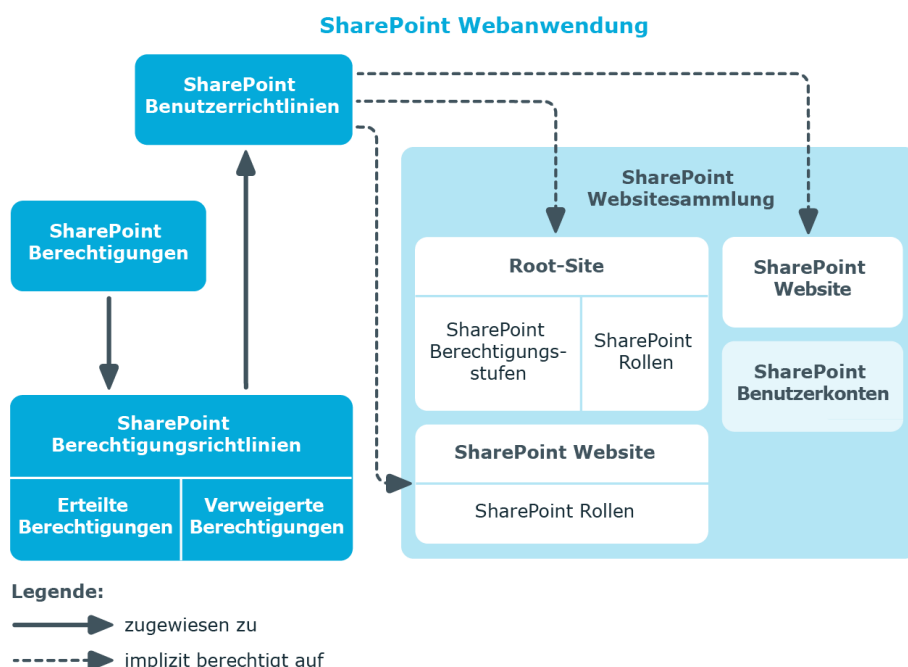
- One Identity Manager Konfigurationshandbuch

## Berechtigungen für SharePoint Webanwendungen

In SharePoint können Benutzerrichtlinien definiert werden, um übergreifende Berechtigungen auf alle Websites einer Webanwendung zu gewähren. Diese Benutzerrichtlinien überlagern alle Berechtigungen, die für die Websites speziell definiert wurden. Benutzerrichtlinien basieren auf den Authentifizierungsobjekten, aus denen auch SharePoint Benutzerkonten erzeugt werden. Diese Authentifizierungsobjekte können als Authentifizierungsobjekte an den Benutzerrichtlinien hinterlegt werden.

Benutzerrichtlinien erhalten ihre Berechtigungen über Berechtigungsrichtlinien. In Berechtigungsrichtlinien werden SharePoint Berechtigungen explizit erteilt oder explizit verweigert.

**Abbildung 5: Berechtigungen für SharePoint Webanwendungen über Richtlinien**



Benutzerrichtlinien und Berechtigungsrichtlinien werden für eine Webanwendung definiert. Benutzerrichtlinien werden dadurch implizit auf alle Websites der Webanwendung

berechtigt. Sie können auf einzelne Zonen eingeschränkt werden oder für alle Zonen der Webanwendung gelten.

## SharePoint Berechtigungsrichtlinien

Auf dem Überblicksformular einer Berechtigungsrichtlinie werden die Webanwendung dargestellt sowie die Benutzerrichtlinien, denen die Berechtigungsrichtlinie zugewiesen ist. Es werden alle explizit erteilten und verweigerten Berechtigungen aufgelistet.

### ***Um einen Überblick über eine Berechtigungsrichtlinie zu erhalten***

1. Wählen Sie die Kategorie **SharePoint | Berechtigungsrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Berechtigungsrichtlinie.
3. Wählen Sie die Aufgabe **Überblick über die SharePoint Berechtigungsrichtlinie**.

Für die Berechtigungsrichtlinie "Deny Write" wird als verweigerter Berechtigung die SharePoint Berechtigung "Deny Write" angezeigt. SharePoint fasst damit intern mehrere Einzelberechtigungen zusammen, die nur in der SharePoint Benutzeroberfläche in Einzelberechtigungen aufgelöst werden. Der One Identity Manager bildet die SharePoint-internen Berechtigungen ab. Dadurch erscheint in der One Identity Manager-Oberfläche nur die Berechtigung "Deny Write". Dem One Identity Manager sind die damit verbundenen Einzelberechtigungen nicht bekannt.

## SharePoint Benutzerrichtlinien

Benutzerrichtlinien verfügen über einen dynamischen Fremdschlüssel (Spalte **Authentifizierungsobjekt**), der auf das jeweilige Authentifizierungsobjekt verweist. Verweist der dynamische Fremdschlüssel auf ein Active Directory oder LDAP Benutzerkonto, kann zusätzlich eine Identität zugeordnet werden.

Jede Benutzerrichtlinie repräsentiert ein Objekt aus einem Authentifizierungssystem. Dieses Objekt kann eine Gruppe oder ein Benutzer sein.

### ***Um die Stammdaten einer Benutzerrichtlinie zu bearbeiten***

1. Wählen Sie die Kategorie **SharePoint | Benutzerrichtlinien**.
2. Wählen Sie in der Ergebnisliste die SharePoint Rolle. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Erfassen Sie auf dem Stammdatenformular die benötigten Daten.
4. Speichern Sie die Änderungen.

Für Benutzerrichtlinien werden die folgenden Stammdaten abgebildet.



**Tabelle 36: Stammdaten einer Benutzerrichtlinie**

<b>Eigenschaft</b>	<b>Beschreibung</b>
Anzeigename	Anzeigename der Benutzerrichtlinie.
Benutzerkonto	Angabe, ob das Authentifizierungsobjekt der Benutzerrichtlinie ein Benutzerkonto ist.
Anmeldename	Anmeldename der Benutzerrichtlinie. Er wird über eine Bildungsregeln ermittelt.
Systemkonto	Angabe, ob die Benutzerrichtlinie in der SharePoint-Umgebung als Systemkonto geführt wird.
Identität	<p>Identität, welche die Benutzerrichtlinie verwendet. Wenn ein Authentifizierungsobjekt zugeordnet ist, wird die verbundene Identität per Bildungsregel über das Authentifizierungsobjekt ermittelt. Wenn kein Authentifizierungsobjekt zugeordnet ist, kann die Identität manuell zugeordnet werden.</p> <p>Eine Identität kann nur zugeordnet werden, wenn die Option <b>Benutzerkonto</b> aktiviert ist.</p>
Webanwendung	Eindeutige Kennung der Webanwendung, für welche die Benutzerrichtlinie eingerichtet wurde.
Zone	Eindeutige Kennung der SharePoint Zone, für welche die Benutzerrichtlinie gültig ist.
Authentifizierungsobjekt	<p>Authentifizierungsobjekt, welches die Benutzerrichtlinie referenziert. Jede Benutzerrichtlinie repräsentiert ein Objekt aus einem Authentifizierungssystem, dem die SharePoint-Installation vertraut. Wenn dieses Authentifizierungssystem als Zielsystem im One Identity Manager verwaltet wird, kann das zur Authentifizierung genutzte Objekt an der Benutzerrichtlinie als Authentifizierungsobjekt hinterlegt werden.</p> <p>Das Authentifizierungsobjekt wird bei der Synchronisation automatisch zugeordnet. Wenn die Option <b>Benutzerkonto</b> aktiviert ist, können folgende Authentifizierungsobjekte zugeordnet sein:</p> <ul style="list-style-type: none"> <li>• Active Directory Benutzerkonten</li> <li>• LDAP Benutzerkonten</li> </ul> <p>Wenn die Option <b>Benutzerkonto</b> deaktiviert ist, können folgende Authentifizierungsobjekte zugeordnet sein:</p> <ul style="list-style-type: none"> <li>• Active Directory Gruppen</li> <li>• LDAP Gruppen</li> </ul>

**HINWEIS:** Wenn das Authentifizierungsobjekt, das einer SharePoint Benutzerrichtlinie zugeordnet ist, aus der One Identity Manager-Datenbank gelöscht wird, wird der Verweis

auf das Authentifizierungsobjekt von der Benutzerrichtlinie entfernt. Gegebenenfalls zugeordnete Identitäten bleiben zugeordnet.

## Globale Benutzerrichtlinien

Globale Benutzerrichtlinien sind Benutzerrichtlinien, die für alle Zonen gültig sind. Sie werden in der Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | Globale Benutzerrichtlinien** abgebildet.

## Zonenspezifische Benutzerrichtlinien

Zonenspezifische Benutzerrichtlinien sind Benutzerrichtlinien, die für eine einzelne Zone einer Webanwendung gültig sind. Sie werden in der Kategorie **SharePoint | Baumdarstellung | <Farm> | Webanwendungen | <Webanwendung> | Zonenspezifische Benutzerrichtlinien | <Zone>** abgebildet.

## Berichte über SharePoint Objekte

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 SharePoint Farmen stehen folgende Berichte zur Verfügung.

**HINWEIS:** Abhängig von den vorhandenen Modulen können weitere Berichte zur Verfügung stehen.

**Tabelle 37: 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 ( <b>Min. Datum</b> ). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Gruppe Rolle	Der Bericht ermittelt alle Rollen, in denen sich Identitäten befinden, welche die ausgewählte Systemberechtigung besitzen.
Übersicht anzeigen	Gruppe Rolle	Der Bericht zeigt einen Überblick über die Systemberechtigung und ihre Zuweisungen.

Bericht	Bereitgestellt für	Beschreibung
Übersicht anzeigen (inklusive Herkunft)	Gruppe Rolle	Der Bericht zeigt einen Überblick über die Systemberechtigung und die Herkunft der zugewiesenen Benutzerkonten.
Übersicht anzeigen (inklusive Historie)	Gruppe Rolle	<p>Der Bericht zeigt einen Überblick über die Systemberechtigung einschließlich eines historischen Verlaufs.</p> <p>Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (<b>Min. Datum</b>). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.</p>
Abweichende Systemberechtigungen anzeigen	Websitesammlung	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)	Website Websitesammlung	<p>Der Bericht liefert alle Benutzerkonten mit ihren Berechtigungen einschließlich eines historischen Verlaufs.</p> <p>Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (<b>Min. Datum</b>). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.</p>
Benutzerkonten mit einer überdurchschnittlichen Anzahl an Systemberechtigungen anzeigen	Websitesammlung	Der Bericht enthält alle Benutzerkonten, die eine überdurchschnittliche Anzahl an Systemberechtigungen besitzen.
Identitäten mit mehreren Benutzerkonten anzeigen	Websitesammlung	Der Bericht zeigt alle Identitäten, die mehrere Benutzerkonten besitzen. Der Bericht enthält eine Risikoeinschätzung.
Systemberechtigungen anzeigen (inklusive Historie)	Website Websitesammlung	<p>Der Bericht zeigt die Systemberechtigungen mit den zugewiesenen Benutzerkonten einschließlich eines historischen Verlaufs.</p> <p>Wählen Sie das Datum, bis zu dem die</p>

Bericht	Bereitgestellt für	Beschreibung
		Historie angezeigt werden soll ( <b>Min. Datum</b> ). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Webanwendung Websitesammlung	Der Bericht ermittelt alle Rollen, in denen sich Identitäten befinden, die im ausgewählten Zielsystem mindestens ein Benutzerkonto besitzen.
Ungenutzte Benutzerkonten anzeigen	Websitesammlung	Der Bericht enthält alle Benutzerkonten, die in den letzten Monaten nicht verwendet wurden.
Unverbundene Benutzerkonten anzeigen	Websitesammlung	Der Bericht zeigt alle Benutzerkonten, denen keine Identität zugeordnet ist.

## Verwandte Themen

- [Übersicht aller Zuweisungen](#) auf Seite 165

# 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 Identitäten 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 Identitäten befinden, die diese Ressource besitzen.
- Wird der Bericht für eine Gruppe oder andere Systemberechtigung erstellt, werden alle Rollen ermittelt, in denen sich Identitäten befinden, die diese Gruppe oder Systemberechtigung besitzen.
- Wird der Bericht für eine Complianceregel erstellt, werden alle Rollen ermittelt, in denen sich Identitäten befinden, die diese Complianceregel verletzen.

- Wird der Bericht für eine Abteilung erstellt, werden alle Rollen ermittelt, in denen die Identitäten der gewählten Abteilung ebenfalls Mitglied sind.
- Wird der Bericht für eine Geschäftsrolle erstellt, werden alle Rollen ermittelt, in denen die Identitäten 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 Identitäten mit dem ausgewählten Basisobjekt befinden.





Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Identitäten 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 Identitäten 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 Identitäten zur Nachverfolgung speichern können. Dabei wird eine neue Geschäftsrolle erstellt und die Identitäten werden der Geschäftsrolle zugeordnet.

### Abbildung 6: Symbolleiste des Berichts Übersicht aller Zuweisungen



Tabelle 38: 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.

## Konfigurationsparameter für die Verwaltung einer SharePoint-Umgebung

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

**Tabelle 39: Konfigurationsparameter**

Konfigurationsparameter	Beschreibung
TargetSystem   SharePoint	<p>Der Bereich SharePoint wird unterstützt. Der Parameter ist ein präprozessorrelevanter Konfigurationsparameter. Die Aktivierung oder Deaktivierung des Konfigurationsparameters erfordert eine Kompilierung der Datenbank.</p> <p>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 <i>One Identity Manager Konfigurationshandbuch</i>.</p>
TargetSystem   SharePoint   Accounts	<p>Parameter zur Konfiguration von SharePoint Benutzerkonten. Wenn der Parameter aktiviert ist, können die Einstellungen für SharePoint Benutzerkonten konfiguriert werden.</p>
TargetSystem   SharePoint   Accounts   MailTemplateDefaultValues	<p>Der Konfigurationsparameter enthält die Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden.</p>
TargetSystem   SharePoint	<p>Der Konfigurationsparameter enthält die Standard-E-Mail-</p>

Konfigurationsparameter	Beschreibung
DefaultAddress	Adresse für Benachrichtigungen, wenn im Zielsystem Aktionen fehlschlagen.
TargetSystem   SharePoint   MaxFullsyncDuration	Angabe der maximalen Laufzeit für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor.
TargetSystem   SharePoint   PersonAutoDefault	Anhand des angegebenen Modus erfolgt die automatische Identitätenzuordnung für Benutzerkonten, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem   SharePoint   PersonAutoFullsync	Modus für die automatische Identitätenzuordnung für Benutzerkonten, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
QER   ITShop   AutoPublish   SPSGroup	<p>Präprozessorrelevanter Konfigurationsparameter zur Steuerung der automatischen Übernahme von SharePoint Gruppen in den IT Shop. Ist der Parameter aktiviert, werden alle Gruppen automatisch als Produkte dem IT Shop zugewiesen. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.</p> <p>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 <i>One Identity Manager Konfigurationshandbuch</i>.</p>
QER   ITShop   AutoPublish   SPSGroup   ExcludeList	<p>Auflistung aller SharePoint Gruppen, für die keine automatische Zuordnung zum IT Shop erfolgen soll. Jeder Eintrag ist Bestandteil eines regulären Suchmusters und unterstützt die Notation für reguläre Ausdrücke.</p> <p>Beispiel:</p> <pre>.*Administrator.* Exchange.* .*Admins .*Operators II S_IUSRS</pre>



## Standardprojektvorlage für SharePoint

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 40: Abbildung der SharePoint Schematypen auf Tabellen im One Identity Manager Schema**

Schematyp im SharePoint	Tabelle im One Identity Manager Schema
SPAlternateUrl	SPSAlternateURL
SPClaimProvider	SPSClaimProvider
SPFarm	SPSFarm
SPGroup	SPSGroup
SPLanguage	SPSLanguage
SPPolicy	SPSPolicyUser
SPPolicyRole	SPSPolicyRole
SPPrefix	SPSPrefix
SPQuotaTemplate	SPSQuota
SPRoleDefinition	SPSRole
RoleAssignment	SPSRIAsgn

<b>Schematyp im SharePoint</b>	<b>Tabelle im One Identity Manager Schema</b>
SPSite	SPSSite
SPUser	SPSUser
SPWeb	SPSWeb
SPWebApplication	SPSWebApplication
SPWebTemplate	SPSWebTemplate

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

## Kontaktieren Sie uns

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

## Technische Supportressourcen

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

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

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

## A

- Active Directory Benutzerkonto
  - SharePoint
    - Authentifizierungsobjekt 96
- Active Directory Domäne
  - SharePoint
    - Authentifizierungsobjekt 96
  - SharePoint Synchronisation 83
- Active Directory Gruppe
  - SharePoint
    - Authentifizierungsobjekt 96
- alternative URL 52
- Anmeldung 10
- Anwendungsrolle
  - Zielsystemverantwortliche 60
- Architektur 9
- Ausschlussdefinition 137, 156
- Ausstehendes Objekt 37
- Authentifizierung
  - Authentifizierungsmodus 51
  - forderungsbasiert (claims based) 12
- Authentifizierungsmodus 51
- Authentifizierungsobjekt 96
- Automatisierungsgrad 67

## B

- Basisobjekt 33, 41
  - erstellen 32
- Benutzer 10
  - Synchronisation 15
- Benutzerkonto 96
  - administratives Benutzerkonto 98

- Administrator 103, 107
- Anmeldename 103, 107, 116
- Anzahl Gruppenmitgliedschaften (Bericht) 163
- Auditor 103, 107
- Authentifizierungsmodus 116
- Authentifizierungsobjekt 96, 103, 107, 116
- Authentifizierungssystem 103, 107
  - automatisch erstellen 62
- Bildungsregel anpassen 116
- Bildungsregeln ausführen 72
- einrichten 102
- Gruppe zuweisen 113, 131
- Identität 98, 103, 107
- Identität zuordnen 107, 116
- Kategorie 140
- Kategorie zuordnen 103, 107
- löschen 120
- Löschverzögerung 120
- mehrere je Identität 96
- privilegiertes Benutzerkonto 98, 103, 107
- Rechte für die Synchronisation 15
- Risikoindex 103, 107
- Rolle zuweisen 114
- Rollenzuweisung 93
- SharePoint Rolle zuweisen 152
- sperrern 120
- Standardbenutzerkonto 98
- Typ 98
- Überblick 113

- zurückholen 120
- Zusatzeigenschaft zuweisen 115
- Benutzerpräfix 51
- Benutzerrichtlinie 160
  - Active Directory Benutzerkonto 160
  - Authentifizierungsobjekt 160
  - globale 162
  - Identität zuordnen 160
  - Systemkonto 160
  - Webanwendung 160
  - Zone 160
  - zonenspezifische 162
- Berechtigung 53
  - Berechtigungsstufe zuweisen 53
  - zulässige Berechtigung 53, 86
    - synchronisieren 28
- Berechtigungsrichtlinie 53, 160
  - erteilte Berechtigung 160
  - Objekttypen für die Synchronisation 160
  - verweigerte Berechtigung 160
- Berechtigungsstufe 53, 144-145
  - an Benutzerkonten zuweisen 145
  - an Gruppen zuweisen 145
  - Berechtigung zuweisen 146
  - löschen 158
  - Rollendefinition 123, 146
  - Überblicksformular 146
  - Website 145
  - zulässige Berechtigung
    - synchronisieren 147
- Bericht
  - Übersicht aller Zuweisungen 165
  - Websitesammlung 163

- Bestellung
  - Berechtigungen 143
  - Gruppen 143
  - Gruppenmitgliedschaft 144
- Bildungsregel
  - IT Betriebsdaten ändern 72

## E

- Einzelobjekt synchronisieren 45
- Einzelobjektsynchronisation 41, 45
  - beschleunigen 42
- Erweitertes Schema 32

## F

- Farm
  - Domäne 83
  - einrichten 83
  - Zielsystemverantwortliche 83

## G

- Gruppe
  - abweichende (Bericht) 163
  - an Abteilung zuweisen 128
  - an Geschäftsrolle zuweisen 130
  - an Kostenstelle zuweisen 128
  - an Standort zuweisen 128
  - ausschließen 137
  - Benutzerkonto zuweisen 128, 131
  - bestellen 143-144
  - Eigentümer 126
  - einrichten 125
  - Gruppenmitgliedschaft 131
  - in IT Shop aufnehmen 133

- in IT Shop aufnehmen  
    (automatisch) 135
- in Systemrolle aufnehmen 132
- Kategorie 140
- Kategorie zuordnen 126
- löschen 142
- Risikoindex 126
- Rollenzuweisung 93
- SharePoint Rolle zuweisen 132
- über IT Shop bestellen 126
- Überblicksformular 137
- Vererbung über Kategorien 89
- Vererbung über Systemrollen 132
- wirksam 137
- Zusatzeigenschaft zuweisen 142
- Gruppenpräfix 51

## I

- Identität
  - Anzahl Benutzerkonten (Bericht) 163
- Identitätenzuordnung
  - automatisch 116
  - entfernen 119
  - manuell 119
  - Suchkriterium 118
- IT Betriebsdaten
  - ändern 72
- IT Shop Regal
  - Gruppen zuweisen 133
  - Kontendefinitionen zuweisen 77
  - SharePoint Rollen zuweisen 154

## J

- Jobserver
  - Eigenschaften 55
  - Lastverteilung 42

## K

- Kategorie 89
- Konfigurationsparameter 167
- Konnektor 9
- Kontendefinition 62
  - an Systemrollen zuweisen 77
  - in IT Shop aufnehmen 77
- Kontingent 54

## L

- Lastverteilung 42
- LDAP Benutzerkonto
  - SharePoint
    - Authentifizierungsobjekt 96
- LDAP Domäne
  - SharePoint
    - Authentifizierungsobjekt 96
    - SharePoint Synchronisation 83
- LDAP Gruppe
  - SharePoint
    - Authentifizierungsobjekt 96

## M

- Mitgliedschaft
  - Änderung provisionieren 39

## O

### Objekt

- ausstehend 37
- publizieren 37
- sofort löschen 37

### Offline-Modus 47

## P

### Präfix 12, 51-52

- Website erstellen 91

### Produkteigner 135

- Gruppe bestellen 143

### Projektvorlage 169

### Provider 12, 86

### Provisionierung

- beschleunigen 42
- Mitgliederliste 39

## R

### Relative URL 52

### Revisionsfilter 37

### Rolle

- Abbildung im One Identity Manager 144
- an Abteilung zuweisen 150
- an Geschäftsrolle zuweisen 151
- an Kostenstelle zuweisen 150
- an Standort zuweisen 150
- ausschließen 156
- Benutzerkonto zuweisen 149, 152
- Berechtigung vererben 123
- Berechtigungsstufe 123, 147
- Gruppe zuweisen 153

- in IT Shop aufnehmen 154

- in Systemrolle aufnehmen 153

- löschen 158

- Risikoindex 147

- Rollendefinition 93, 123

- Rollenzuweisung 123, 152-153

- über IT Shop bestellen 147

- Überblicksformular 156

- Vererbung über hierarchische Rollen 149

- Vererbung über Systemrollen 153

- Website 147

- wirksam 156

### Root-Site 90

- Website 90

- Websitesammlung 88

## S

### Schema

- aktualisieren 35
- Änderungen 35
- komprimieren 35

### Scope 30

### Serverfarmkonto 15

### Serverfunktion 58

### SharePoint Rolle

- Zusatzeigenschaft zuweisen 157

### Sprache 53-54

### Startkonfiguration 33

### Synchronisation

- beschleunigen 37
- konfigurieren 21
- Microsoft.SharePoint.dll 16
- Provider 12
- Rechte 15

- starten 21
- Synchronisationsserver
  - konfigurieren 16
- Verbindungsdaten 21
- verhindern 44
- verschiedene Farmen 32
- Voraussetzungen 14
- Synchronisationsanalysebericht 43
- Synchronisationskonfiguration
  - anpassen 30-32
  - Remoteverbindung 31-32
- Synchronisationsprojekt
  - bearbeiten 84
  - deaktivieren 44
  - einrichten 21
  - Projektvorlage 169
- Synchronisationsprotokoll 29
- Synchronisationsrichtung
  - In das Zielsystem 31
- Synchronisationsserver
  - bearbeiten 54
  - Serverfunktion 58
- Synchronisationsworkflow
  - erstellen 31
- Systemverbindung
  - aktives Variablenset 35
  - ändern 33

## U

- ungenutzte Benutzerkonten
  - (Bericht) 163
- unverbundene Benutzerkonten
  - (Bericht) 163
- URL
  - Präfix 52

- Website 91-92
- Websitesammlung 88

## V

- Variable 30
- Variablenset 32-33
  - aktiv 35
- Verbindungsparameter 21, 30, 32
- Verbindungsparameter umwandeln 33

## W

- Webanwendung 86
  - alternative URL 52
  - Benutzerrichtlinie 86, 159
  - Berechtigungsrichtlinie 86, 159
  - Forderungsauthentifizierung 86
  - übergreifende Berechtigungen 159
  - zulässige Berechtigungen 53, 86
  - zulässige Provider 86
- Website 90
  - anonymer Zugriff 90
  - Autor 90
  - erstellen 94
  - Präfix 91
  - Rollendefinition 90, 93
  - Rollenzuweisung 90, 93
  - Root-Site 90
    - Berechtigungen vererben 93, 123
  - über IT Shop bestellen 94
  - untergeordnete 123
  - URL 91-92
    - öffnen 91
  - Webvorlage 92



- Websitesammlung 87
  - Administrator 88
  - erstellen 94
  - Identitätszuordnung 118
  - Kategorie 140
  - Kategorien festlegen 89
  - Kontendefinition 88
  - Kontingent 54
  - Root-Site 88
    - Berechtigungen vererben 93, 123
  - Server 88
  - über IT Shop bestellen 94
  - URL 88
- Webvorlage 53
  - Website erstellen 92
- Workflow 31

## **Z**

- Zeitplan
  - deaktivieren 44
- Zielsystem
  - nicht verfügbar 47
- Zielsystemabgleich 37
- Zielsystemschemata 32
- Zielsystemverantwortlicher 60
  - zuordnen 83
- Zone 52
  - Benutzerrichtlinie 160
- Zusatzeigenschaft
  - Benutzerkonto 115
  - Gruppe zuweisen 142
  - SharePoint Rolle zuweisen 157