Copyright 2019 One Identity LLC.
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser’s personal use without the written permission of One Identity LLC.

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

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

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

**Patents**

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

**Trademarks**

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

**Legend**

![WARNING] A WARNING icon indicates a potential for property damage, personal injury, or death.

![CAUTION] A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

![IMPORTANT, NOTE, TIP, MOBILE, or VIDEO] An information icon indicates supporting information.

One Identity Manager Administration Guide for Connecting to SAP R/3
Updated - August 2019
Version - 8.1.1
Contents

Managing SAP R/3 environments ................................................................. 8
Architecture overview .................................................................................. 8
One Identity Manager users for managing an SAP R/3 environment .......... 11

Setting up synchronization with an SAP R/3 environment ....................... 13
Users and permissions for synchronizing with an SAP R/3 environment .... 14
Installing the One Identity Manager Business Application Programing Interface ..... 16
  Uninstalling BAPI transports .................................................................... 17
Setting up the synchronization server ......................................................... 18
Creating a synchronization project for initial synchronization of an SAP client ... 21
Special features of synchronizing with a CUA central system .................. 32
  Excluding a child system from synchronization ...................................... 33
Displaying synchronization results .............................................................. 35
Customizing synchronization configuration ................................................. 35
  How to configure synchronization in the SAP R/3 environment ............. 37
  Configuring synchronization of different clients .................................... 37
Updating schemas ....................................................................................... 38
Adding other schema types ........................................................................ 39
Creating a schema extension file ............................................................... 40
  Defining tables ......................................................................................... 42
  Defining functions .................................................................................... 45
  Defining schema types ............................................................................ 46
Speeding up synchronization with revision filtering .................................. 49
Synchronizing collective roles .................................................................... 50
Restricting synchronization objects using user permissions .................. 51
Post-processing outstanding objects ........................................................ 51
Configuring the provisioning of memberships ......................................... 54
Help for the analysis of synchronization issues ....................................... 55
Disabling synchronization .......................................................................... 55

Basic data for managing an SAP R/3 environment .................................... 57
Setting up account definitions ................................................................... 58
  Creating an account definition .................................................................. 59
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master data for an account definition</td>
<td>59</td>
</tr>
<tr>
<td>Creating manage levels</td>
<td>62</td>
</tr>
<tr>
<td>Master data for a manage level</td>
<td>63</td>
</tr>
<tr>
<td>Creating a mapping rule for IT operating data</td>
<td>64</td>
</tr>
<tr>
<td>Entering the IT operating data</td>
<td>66</td>
</tr>
<tr>
<td>Modify IT operating data</td>
<td>67</td>
</tr>
<tr>
<td>Assigning account definitions to employees</td>
<td>68</td>
</tr>
<tr>
<td>Assigning account definitions to departments, cost centers, and locations</td>
<td>69</td>
</tr>
<tr>
<td>Assigning an account definition to business roles</td>
<td>70</td>
</tr>
<tr>
<td>Assigning account definitions to all employees</td>
<td>70</td>
</tr>
<tr>
<td>Assigning account definitions directly to employees</td>
<td>71</td>
</tr>
<tr>
<td>Assigning account definitions to system roles</td>
<td>71</td>
</tr>
<tr>
<td>Adding account definitions in the IT Shop</td>
<td>72</td>
</tr>
<tr>
<td>Assigning account definitions to a target system</td>
<td>73</td>
</tr>
<tr>
<td>Deleting an account definition</td>
<td>74</td>
</tr>
<tr>
<td>Basic data for user account administration</td>
<td>76</td>
</tr>
<tr>
<td>User account types</td>
<td>76</td>
</tr>
<tr>
<td>External identifier types</td>
<td>77</td>
</tr>
<tr>
<td>Parameters</td>
<td>78</td>
</tr>
<tr>
<td>Printers</td>
<td>78</td>
</tr>
<tr>
<td>Cost centers</td>
<td>78</td>
</tr>
<tr>
<td>Start menus</td>
<td>79</td>
</tr>
<tr>
<td>Companies</td>
<td>79</td>
</tr>
<tr>
<td>Login languages</td>
<td>79</td>
</tr>
<tr>
<td>Security policies</td>
<td>79</td>
</tr>
<tr>
<td>Communication types</td>
<td>80</td>
</tr>
<tr>
<td>Licenses</td>
<td>80</td>
</tr>
<tr>
<td>Special versions</td>
<td>81</td>
</tr>
<tr>
<td>Password policies for SAP user accounts</td>
<td>81</td>
</tr>
<tr>
<td>Predefined password policies</td>
<td>82</td>
</tr>
<tr>
<td>Using a password policy</td>
<td>83</td>
</tr>
<tr>
<td>Editing password policies</td>
<td>85</td>
</tr>
<tr>
<td>Custom scripts for password requirements</td>
<td>88</td>
</tr>
<tr>
<td>Excluded list for passwords</td>
<td>90</td>
</tr>
<tr>
<td>Checking a password</td>
<td>91</td>
</tr>
</tbody>
</table>
Testing generation of a password ................................................................. 91
Initial password for new SAP user accounts ................................................. 91
Email notifications about login data ............................................................. 93
Editing a server ......................................................................................... 94
Master data for a Job server ....................................................................... 95
Specifying server functions ....................................................................... 98
Target system managers ........................................................................... 99

**SAP systems** .......................................................................................... 102

**SAP clients** ............................................................................................. 103
General master data for an SAP client ....................................................... 103
Specifying categories for inheriting SAP groups, SAP roles and SAP profiles 105
Editing a synchronization project ............................................................... 106

**SAP user accounts** ................................................................................ 107
Linking user accounts to employees ......................................................... 107
Supported user account types .................................................................. 108
Central user administration in One Identity Manager ............................. 112
Entering SAP user account master data .................................................... 114
  General master data of an SAP user account ........................................... 115
  SAP user account login data ................................................................. 119
  Telephone numbers .............................................................................. 120
  Fax numbers ........................................................................................ 121
  Email addresses ................................................................................... 122
  Fixed values for an SAP user account ................................................... 123
  Measurement data ................................................................................ 124
  Assigning parameters .......................................................................... 124
  SNC data for an SAP user account ....................................................... 125
Additional tasks for managing SAP user accounts .................................... 125
  Overview of the SAP user account ......................................................... 125
  Changing the manage level of an SAP user account ............................... 125
  Assigning SAP groups and SAP profiles directly to an SAP user account 126
  Assigning SAP roles directly to an SAP user account ............................. 127
  Assigning structural profiles ................................................................. 128
  Granting access to clients of a central user administration .................... 129
  SAP Licenses assign ............................................................................. 130
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Locking user accounts</td>
<td>131</td>
</tr>
<tr>
<td>Assigning extended properties</td>
<td>132</td>
</tr>
<tr>
<td>Automatic assignment of employees to SAP user accounts</td>
<td>132</td>
</tr>
<tr>
<td>Editing the search criteria for automatic employee assignment</td>
<td>135</td>
</tr>
<tr>
<td>Locking SAP user accounts</td>
<td>137</td>
</tr>
<tr>
<td>Deleting and restoring SAP user accounts</td>
<td>139</td>
</tr>
<tr>
<td>Entering external user identifiers for an SAP user account</td>
<td>140</td>
</tr>
<tr>
<td><strong>SAP groups, SAP roles and SAP profiles</strong></td>
<td>142</td>
</tr>
<tr>
<td>Editing the master data for SAP groups, SAP roles, and SAP profiles</td>
<td>142</td>
</tr>
<tr>
<td>General master data for SAP groups</td>
<td>143</td>
</tr>
<tr>
<td>General master data for SAP roles</td>
<td>145</td>
</tr>
<tr>
<td>General master data for SAP profiles</td>
<td>146</td>
</tr>
<tr>
<td>Assigning SAP groups, SAP roles, and SAP profiles to SAP user accounts</td>
<td>148</td>
</tr>
<tr>
<td>Assigning SAP groups, SAP roles, and SAP profiles to organizations</td>
<td>148</td>
</tr>
<tr>
<td>Assigning SAP groups, SAP roles, and SAP profiles to business roles</td>
<td>150</td>
</tr>
<tr>
<td>Assigning SAP user accounts directly to SAP groups, and SAP profiles</td>
<td>152</td>
</tr>
<tr>
<td>Assigning SAP user accounts directly to SAP roles</td>
<td>153</td>
</tr>
<tr>
<td>Adding SAP groups, SAP roles, and SAP profiles in system roles</td>
<td>154</td>
</tr>
<tr>
<td>Adding SAP groups, SAP roles, and SAP profiles to the IT Shop</td>
<td>156</td>
</tr>
<tr>
<td>Validity period of role assignments</td>
<td>158</td>
</tr>
<tr>
<td>Assigning and passing on SAP profiles and SAP roles to SAP user accounts</td>
<td>160</td>
</tr>
<tr>
<td>Additional tasks for managing SAP groups, SAP roles, and SAP profiles</td>
<td>160</td>
</tr>
<tr>
<td>Overview of SAP groups, SAP roles, and SAP profiles</td>
<td>161</td>
</tr>
<tr>
<td>Effectiveness of SAP groups, SAP roles, and SAP profiles</td>
<td>161</td>
</tr>
<tr>
<td>Inheriting SAP groups, SAP roles, and SAP profiles based on categories</td>
<td>164</td>
</tr>
<tr>
<td>Assigning extended properties to SAP groups, SAP roles and SAP profiles</td>
<td>166</td>
</tr>
<tr>
<td>SAP Showing authorizations</td>
<td>167</td>
</tr>
<tr>
<td>Calculating the validity date of inherited role assignments</td>
<td>168</td>
</tr>
<tr>
<td><strong>SAP Products</strong></td>
<td>170</td>
</tr>
<tr>
<td>General master data for an SAP product</td>
<td>171</td>
</tr>
<tr>
<td>Assigning SAP products to employees</td>
<td>173</td>
</tr>
<tr>
<td>Assigning SAP products to organizations</td>
<td>173</td>
</tr>
<tr>
<td>Assigning SAP products to business roles</td>
<td>174</td>
</tr>
<tr>
<td>Assigning SAP products directly to employees</td>
<td>175</td>
</tr>
</tbody>
</table>
Adding SAP products in system roles .................................................. 175
Adding SAP products to the IT Shop .................................................. 176
Additional tasks for managing SAP products ........................................ 177
Overview of the SAP product ............................................................... 178
Assigning SAP groups, SAP roles and SAP profiles to an SAP product .... 178
Assigning account definitions to an SAP product .................................. 179
Assigning subscribable reports to SAP products .................................... 180
Assigning extended properties to an SAP product ................................. 180
Editing conflicting system roles ............................................................ 181

Providing system measurement data .................................................... 182
Mapping the measurement data ............................................................. 183
Entering licenses for SAP user accounts ............................................... 185
Determining licenses using SAP roles and SAP profiles ......................... 186
  Determining the rating of an SAP user account .................................... 187
  Transferring calculated licenses ....................................................... 189

Reports about SAP systems .................................................................. 191
Overview of all assignments .................................................................. 192

Appendix: Configuration parameters for managing an SAP R/3 environment .................................................... 194

Appendix: Default project templates for synchronizing an SAP R/3 environment .................................................... 199
Project template for client without CUA ................................................. 199
Project template for the CUA central system ......................................... 201
Project template for CUA subsystems .................................................... 202

Appendix: Referenced SAP R/3 tables and BAPI calls .......................... 203

Appendix: Example of a schema extension file ....................................... 206

About us ............................................................................................... 210
Contacting us ....................................................................................... 210
Technical support resources ................................................................... 210

Index ...................................................................................................... 211
Managing SAP R/3 environments

One Identity Manager offers simplified user administration for SAP R/3 environments. The One Identity Manager concentrates on setting up and processing user accounts as well as groups, roles, and profiles assignments. External identifiers and parameters can also be assigned to user accounts. The necessary data for system measurement is also mapped. The system measurement data is available in One Identity Manager, but the measurement itself takes place in the SAP R/3 environment.

One Identity Manager provides company employees with the necessary user accounts. For this, you can use different mechanisms to connect employees to their user accounts. You can also manage user accounts independently of employees and therefore set up administrator user accounts.

Groups, roles and profiles are mapped in the One Identity Manager, in order to provide the necessary permissions for user accounts. Groups, roles, and profiles can be grouped into products and assigned to employees. One Identity Manager ensures that the right group memberships are created for the employee’s user account.

If user accounts are managed through the central user administration (CUA) in SAP R/3, access to the child client can be guaranteed to or withdrawn from user accounts in One Identity Manager.

Architecture overview

The following servers in One Identity Manager play a role in managing an SAP R/3 environment:

- SAP R/3 application server
  Application server on which synchronization is executed

- SAP R/3 database server
  Server on which the SAP R/3 application database is installed.
- **Synchronization server**
  The synchronization server for synchronizing the One Identity Manager database with the SAP R/3 system. The One Identity Manager Service is installed on this server with the SAP R/3 connector. The synchronization server connects to the SAP R/3 application server.

- **SAP R/3 router**
  Router which provides a network port to the SAP connector for communicating with the SAP R/3 application server.

- **SAP R/3 message server**
  Server with which the SAP R/3 connector communicates during login if a direct connection to application servers is not permitted.

The One Identity Manager SAP R/3 connector executes synchronization and provision of data between SAP R/3 and the One Identity Manager database. The SAP R/3 connector uses the SAP connector for Microsoft .NET (NCo 3.0) for 64-bit systems for communicating with the target system.

One Identity Manager is responsible for synchronizing data between the SAP R/3 database and the One Identity Manager Service. The application server ABAP must be installed as a prerequisite for synchronization. An SAP system that is only based on a Java application server cannot be accessed with the SAP R/3 connector.

**Figure 1: Architecture for Synchronization - Direct Communication**
Figure 2: Architecture for Synchronization - Communication through Message Server

Figure 3: Architecture for Synchronization - Communication through Router
One Identity Manager users for managing an SAP R/3 environment

The following users are included in setting up and managing an SAP R/3 environment.

<table>
<thead>
<tr>
<th>User</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target system administrators</td>
<td>Target system administrators must be assigned to the **Target systems</td>
</tr>
<tr>
<td></td>
<td>• Administate application roles for individual target system types.</td>
</tr>
<tr>
<td></td>
<td>• Specify the target system manager.</td>
</tr>
<tr>
<td></td>
<td>• Set up other application roles for target system managers if required.</td>
</tr>
<tr>
<td></td>
<td>• Specify which application roles for target system managers are mutually exclusive.</td>
</tr>
<tr>
<td></td>
<td>• Authorize other employee to be target system administrators.</td>
</tr>
<tr>
<td></td>
<td>• Do not assume any administrative tasks within the target system.</td>
</tr>
<tr>
<td>Target system managers</td>
<td>Target system managers must be assigned to **Target systems</td>
</tr>
<tr>
<td></td>
<td>• Assume administrative tasks for the target system.</td>
</tr>
<tr>
<td></td>
<td>• Create, change or delete target system objects, like user accounts or groups.</td>
</tr>
<tr>
<td></td>
<td>• Edit password policies for the target system.</td>
</tr>
<tr>
<td></td>
<td>• Prepare system entitlements for adding to the IT Shop.</td>
</tr>
<tr>
<td></td>
<td>• Can add employees, who have an other identity than the <strong>Primary identity</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager.</td>
</tr>
<tr>
<td></td>
<td>• Edit the synchronization's target system types and outstanding objects.</td>
</tr>
<tr>
<td></td>
<td>• Authorize other employees within their area of</td>
</tr>
<tr>
<td>User</td>
<td>Task</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
</tr>
</tbody>
</table>
| One Identity Manager administrators | - Create customized permissions groups for application roles for role-based login to administration tools in Designer as required.  
- Create system users and permissions groups for non-role-based login to administration tools in Designer as required.  
- Enable or disable additional configuration parameters in Designer as required.  
- Create custom processes in Designer as required.  
- Create and configure schedules as required.  
- Create and configure password policies as required. |
| Administrators for the IT Shop | Administrators must be assigned to the **Request & Fulfillment | IT Shop | Administrators** application role.  
Users with this application role:  
- Assign system entitlements to IT Shop structures. |
| Administrators for organizations | Administrators must be assigned to the application role **Identity Management | Organizations | Administrators**.  
Users with this application role:  
- Assign system entitlements to departments, cost centers and locations. |
| Business roles administrators | Administrators must be assigned to the application role **Identity Management | Business roles | Administrators**.  
Users with this application role:  
- Assign system entitlements to business roles. |
Setting up synchronization with an SAP R/3 environment

The One Identity Manager supports synchronization with SAP systems for the following versions:

- SAP Web Application Server 6.40
- SAP NetWeaver Application Server 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.31, 7.40 SR 2, 7.41 and 7.50
- SAP ECC 5.0 and 6.0
- SAP S/4HANA On-Premise edition

Central User Administration is supported for all versions named here.

To load SAP R/3 objects into the One Identity Manager database for the first time

1. Prepare a user account with sufficient permissions for synchronizing in SAP R/3.
2. Install the One Identity Manager Business Application Programming Interface in the SAP R/3 system.
3. The One Identity Manager parts for managing SAP R/3 systems are available if "TargetSystem\SAPR3" is set.
   - Check whether the configuration parameter is set in the Designer. Otherwise, set the configuration parameter and compile the database.
   - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
4. Download the installation source for the SAP .Net Connector for .NET 4.0 on x64, with at least version 3.0.15.0.
5. Install and configure a synchronization server and declare the server as Job server in One Identity Manager.
6. Create a synchronization project with the Synchronization Editor.
Detailed information about this topic

- Users and permissions for synchronizing with an SAP R/3 environment on page 14
- Installing the One Identity Manager Business Application Programming Interface on page 16
- Setting up the synchronization server on page 18
- Creating a synchronization project for initial synchronization of an SAP client on page 21

Users and permissions for synchronizing with an SAP R/3 environment

The following users are involved in synchronizing One Identity Manager with SAP R/3.

Table 2: Users for synchronization

<table>
<thead>
<tr>
<th>User</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Identity Manager Service user account</td>
<td>The user account for One Identity Manager Service requires rights to carry out operations at file level, for example, assigning user rights and creating and editing directories and files. The user account must belong to the Domain users group. The user account must have the Login as a service extended user right. The user account requires access rights to the internal web service.</td>
</tr>
</tbody>
</table>

**NOTE:** If One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access rights for the internal web service with the following command line call:

```
netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"
```

The user account needs full access to the One Identity Manager Service installation directory in order to automatically update the One Identity Manager.

In the default installation the One Identity Manager is installed under:

- %ProgramFiles(x86)%\One Identity (on 32-bit operating systems)
- %ProgramFiles%\One Identity (on 64-bit operating systems)
<table>
<thead>
<tr>
<th>User for accessing the target system</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User</strong></td>
<td>You must provide a user account with the following authorizations for full synchronization of SAP R/3 objects with the supplied One Identity Manager default configuration.</td>
</tr>
<tr>
<td></td>
<td>Required authorization objects and their meanings:</td>
</tr>
<tr>
<td></td>
<td>- S_TCODE with a minimum of transaction codes SU01, SU53, PFCG</td>
</tr>
<tr>
<td></td>
<td>- S_ADDRESS1 with activities 01, 02, 03, 06 and valid address groups (min.&quot;BC01&quot;)</td>
</tr>
<tr>
<td></td>
<td>- S_USER_AGR (role maintenance) with activities 02, 03, 22, 78 possibly with restrictions in name ranges (for example &quot;Z**&quot;)</td>
</tr>
<tr>
<td></td>
<td>- S_USER_GRP (group maintenance) with activities 01, 02, 03, 22</td>
</tr>
<tr>
<td></td>
<td>- S_USER_AUT (authorizations) with activities 03, 08</td>
</tr>
<tr>
<td></td>
<td>- S_USER_PRO (profile) with activities 01, 02, 03, 22</td>
</tr>
<tr>
<td></td>
<td>- S_USER_SAS (system specific assignments) with activities 01, 06, 22</td>
</tr>
<tr>
<td></td>
<td>- S_RFC (authorization check by RFC access) with activity 16 at least for function groups ZVI, /VIAENET/ZVI0, /VIAENET/ZVI_L, /VIAENET/Z_HR, SU_USER, SYST, SDTX, RFC1, RFC_METADATA, SDIFORM, SYSU,</td>
</tr>
<tr>
<td></td>
<td>- S_TABU_DIS (use of standard tools like SM30 for maintaining tables) with activity 03</td>
</tr>
<tr>
<td></td>
<td>Apart from the permissions listed, the user account has to get all objects from the authorization classes &quot;ZVIH_AUT&quot;, &quot;ZVIA_AUT&quot;, and &quot;ZVIL_AUT&quot; that are installed by the transport package for synchronization.</td>
</tr>
<tr>
<td></td>
<td>The following authorization objects are required in addition for the child system in order to synchronize central user administration:</td>
</tr>
<tr>
<td></td>
<td>- S_RFC with the function group SUU6</td>
</tr>
<tr>
<td></td>
<td>- S_TCODE with the transaction code SU56</td>
</tr>
</tbody>
</table>

| User for accessing the One Identity Manager database | The **Synchronization** default system user is provided for executing synchronization with an application server. |

**TIP:** The transport file provided by default, "SAPRole.zip", includes a transport package with a role that the base authorization object already possesses. This role can be assigned to the user account. You will find the transport files on the One Identity Manager installation medium in ..\Modules\SAP\dvd\AddOn\Bap1.
The named authorizations are required so that the SAP R/3 connector has read and write access to the SAP R/3 system. If only read access should be permitted, setting up a profile which has executable permission for transactions SU01 and PFCG but prevents writing at activity or field level is recommended.

The user account requires the user type "dialog", "communication", or "system" to load more information.

NOTE: In SAP R/3 versions up to and including SAP Web Application Server 6.40, the password and user input are not case-sensitive. this no longer applies to the password for SAP NetWeaver Application Server 7.0 and later. The password is case sensitive.

All SAP’s own tools that are supplied up to SAP Web Application Server 6.40, apart from the SAP GUI (RFC-SDK, SAP .Net Connector), therefore change the password to capital letters before passing them to SAP R/3. You must set the password in capital letters for the user account used by the SAP .Net Connector to authenticate itself on the SAP R/3 system. If this is done, all the usual tools can be accessed on SAP NetWeaver Application Server 7.0 by RFC.

Related topics

- Appendix: Referenced SAP R/3 tables and BAPI calls on page 203

## Installing the One Identity Manager Business Application Programming Interface

NOTE: The Business Application Programming Interface in One Identity Manager is certified.

Certificates:

- Integration with SAP S/4HANA
- Powered by SAP NetWeaver

For detailed information, see https://www.sapappcenter.com/apps/5513#!overview.

In order to access One Identity Manager data and business processes with the SAP R/3, you must load the Business Application Programming Interface (BAPI) into the SAP R/3 system. You will find the required transport files on the One Identity Manager installation medium in Modules\SAP\dvd\AddOn\Bapi.

TIP: Instead of installing SAPTRANSPORT_70.ZIP, you can install the Assembly Kit T070020759523_0000006.PAT. For more information, see Uninstalling BAPI transports on page 17.

Install the BAPI transport in the following order:
Table 3: BAPI transport

<table>
<thead>
<tr>
<th>Transport</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  SAPRepository.zip</td>
<td>Creates the /VIAENET/ in the SAP system repository.</td>
</tr>
<tr>
<td>2  SAPTable.zip</td>
<td>Defines the table structure for /VIAENET/USERS in the SAP system dictionary.</td>
</tr>
<tr>
<td>3  SAPTRANSPORT_70.ZIP</td>
<td>Contains the functions defined in the /VIAENET/ environment. Select the transport package that suits your SAP system.</td>
</tr>
<tr>
<td></td>
<td>Archive directory UNICODE: Transports for systems that support unicode; transports for copies</td>
</tr>
<tr>
<td></td>
<td>Archive directory NON_UNICODE: Transports for systems not supporting unicode</td>
</tr>
<tr>
<td></td>
<td>Archive directory UNICODE_WORKBENCH: Transports for systems that support unicode; workbench transports</td>
</tr>
</tbody>
</table>

Set the following import options for the transport:

- Overwrite Originals
- Overwrite Objects in Unconfirmed Repairs
- Ignore Non-Matching Component Versions

The SAP R/3 connector uses other BAPI SAP R/3s in parallel. For more information, see Appendix: Referenced SAP R/3 tables and BAPI calls on page 203.

Uninstalling BAPI transports

The SAP Add-On Assembly Kit allows SAP to support deinstallation of a BAPI. An uninstallable Assembly Kit is proved for this.

Prerequisites

- SAP NetWeaver Application Server 7.00 or later
- SAP ECC 6.0
- SAP Add-On Assembly Kit 5.0 or later
- Unicode is supported.

To uninstall a BAPI transport at a later date

- Install the Assembly Kit C360020276329_0000007.PAT instead of the transport file SAPTRANSPORT_70.ZIP.
  You will find the kit on the One Identity Manager installation medium in the directory Modules\SAP\dvd\AddOn\Bapi.
The kit contains the functions that are defined in the /VIAENET/ environment. The kit has the option deinstall_allowed set.

**Related topics**

- Installing the One Identity Manager Business Application Programing Interface on page 16

**Setting up the synchronization server**

To set up synchronization with an SAP R/3 environment, a server has to be available that has the following software installed on it:

- Windows operating system
  Following versions are supported:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later
- Microsoft .NET Framework Version 4.7.2 or later
  
  **NOTE:** Take the target system manufacturer's recommendations into account.
- Windows Installer
- SAP .Net Connector for .NET 4.0 on x64, with at least version 3.0.15.0
- One Identity Manager Service, Synchronization Editor, SAP R/3 connector
  - Install One Identity Manager components with the installation wizard.
    1. Select **Select installation modules with existing database.**
    2. Select the machine role **Server | Job server | SAP R/3.**

**Further requirements**

- Following files must either be in the Global Assemblies Cache (GAC) or in the One Identity Manager installation directory.
  - libicudecnumber.dll
  - rscp4n.dll
  - sapnco.dll
  - sapnco_utils.dll
- Following files must either be in the Global Assemblies Cache (GAC) or in C:\Windows\System32 or in the One Identity Manager's installation directory.
All One Identity Manager service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager.

NOTE: If several target system environments of the same type are synchronized under the same synchronization server, it is useful to set up a Job server for each target system on performance grounds. This avoids unnecessary swapping of connections to target systems because a Job server only has to process tasks of the same type (re-use of existing connections).

Use the One Identity Manager Service to install the Server Installer. The program executes the following steps:

- Setting up a Job server.
- Specifying machine roles and server function for the Job server.
- Remote installation of One Identity Manager Service components corresponding to the machine roles.
- Configuration of One Identity Manager Service.
- Starts the One Identity Manager Service.

NOTE: The program executes remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program. Remote installation is only supported within a domain or a trusted domain.

For remote installation of One Identity Manager Service, you require an administrative workstation on which the One Identity Manager components are installed. For detailed information about installing a workstation, see the One Identity Manager Installation Guide.

To install and configure One Identity Manager Service remotely on a server

1. Start the program Server Installer on your administrative workstation.
2. Enter the valid connection credentials for the One Identity Manager database on the Database connection page.
3. Specify the server on which you want to install One Identity Manager Service on the Server properties page.
   a. Select a Job server from the Server menu.
   - OR -
   To create a new Job server, click Add.
   b. Enter the following data for the Job server.
**Table 4: Job server properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Job server name.</td>
</tr>
<tr>
<td>Queue</td>
<td>Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.</td>
</tr>
<tr>
<td>Full server name</td>
<td>Full server name in accordance with DNS syntax. Example: &lt;Name of servers&gt;.&lt;Fully qualified domain name&gt;</td>
</tr>
</tbody>
</table>

**NOTE:** You can use the Extended option to make changes to other properties for the Job server. You can also edit the properties later with Designer.

5. Select SAP R/3 connector on the Server functions page.
6. Check the One Identity Manager Service configuration on the Service settings page.
   
   **NOTE:** The initial service configuration is predefined already. If further changes need to be made to the configuration, you can do this later with the Designer. For detailed information about configuring the service, see the One Identity Manager Configuration Guide.

7. To configure remote installations, click Next.
8. Confirm the security prompt with Yes.
9. Select the directory with the install files on Select installation source.
10. Select the file with the private key on the page Select private key file.

   **NOTE:** This page is only displayed when the database is encrypted.
11. Enter the service's installation data on the Service access page.

**Table 5: Installation data**

<table>
<thead>
<tr>
<th>Data</th>
<th>Description serviceProvider on which to install and start the service from.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer</td>
<td>Server on which to install and start the service from.</td>
</tr>
</tbody>
</table>

**To select a server**
- Enter a name for the server.
<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service account</td>
<td>User account data for the One Identity Manager Service.</td>
</tr>
<tr>
<td></td>
<td>To enter a user account for the One Identity Manager Service</td>
</tr>
<tr>
<td></td>
<td>- Set the option Local system account.</td>
</tr>
<tr>
<td></td>
<td>This starts the One Identity Manager Service under the NT AUTHORITY\SYSTEM account.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>Enter user account, password and password confirmation.</td>
</tr>
<tr>
<td>Installation</td>
<td>Data for the administrative user account to install the service.</td>
</tr>
<tr>
<td>account</td>
<td>To enter an administrative user account for installation</td>
</tr>
<tr>
<td></td>
<td>- Enable Advanced.</td>
</tr>
<tr>
<td></td>
<td>- Enable Current user.</td>
</tr>
<tr>
<td></td>
<td>This uses the user account of the current user.</td>
</tr>
<tr>
<td></td>
<td>- OR -</td>
</tr>
<tr>
<td></td>
<td>Enter user account, password and password confirmation.</td>
</tr>
</tbody>
</table>

12. Click **Next** to start installing the service.

   Installation of the service occurs automatically and may take some time.

13. Click **Finish** on the last page of Server Installer.

   ! **NOTE:** The service is entered with the name **One Identity Manager Service** in the server service management.

### Creating a synchronization project for initial synchronization of an SAP client

Use Synchronization Editor to configure synchronization between the One Identity Manager database and SAP R/3 environment. The following describes the steps for initial configuration of a synchronization project.

After the initial configuration, you can customize and configure workflows within the synchronization project. Use the workflow wizard in the Synchronization Editor for this. The Synchronization Editor also provides different configuration options for a synchronization project.

Have the following information available for setting up a synchronization project.
Table 6: Information Required for Setting up a Synchronization Project

<table>
<thead>
<tr>
<th>Data</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP R/3 application server</td>
<td>Name of the application server used to RFC communication.</td>
</tr>
<tr>
<td>System number</td>
<td>Number of the SAP R/3 system for connecting the SAP connector.</td>
</tr>
<tr>
<td>System ID</td>
<td>System ID of this SAP system.</td>
</tr>
<tr>
<td>Client</td>
<td>Number of the client to be synchronized. You need the central system's</td>
</tr>
<tr>
<td></td>
<td>client number to synchronize central user administration (CUA).</td>
</tr>
<tr>
<td>Login name and password</td>
<td>The name and password of the user account used by the SAP R/3 connector to</td>
</tr>
<tr>
<td></td>
<td>log in to the SAP R/3 system. Make a user account available with sufficient</td>
</tr>
<tr>
<td></td>
<td>permissions. If the network connection must be secure, you require the</td>
</tr>
<tr>
<td></td>
<td>user account’s SNC name.</td>
</tr>
<tr>
<td>Login language</td>
<td>Login language for logging the SAP R/3 connection into the SAP R/3 system.</td>
</tr>
<tr>
<td>Synchronization server</td>
<td>All One Identity Manager Service actions are executed against the</td>
</tr>
<tr>
<td></td>
<td>target system environment on the synchronization server. Data entries</td>
</tr>
<tr>
<td></td>
<td>required for synchronization and administration with the One Identity</td>
</tr>
<tr>
<td></td>
<td>Manager database are processed by the synchronization server.</td>
</tr>
<tr>
<td></td>
<td>Installed components:</td>
</tr>
<tr>
<td></td>
<td>• SAP .Net Connector for .NET 4.0 on x64, with at least version 3.0.15.0</td>
</tr>
<tr>
<td></td>
<td>• One Identity Manager Service (started)</td>
</tr>
<tr>
<td></td>
<td>• Synchronization Editor</td>
</tr>
<tr>
<td></td>
<td>• SAP R/3 connector</td>
</tr>
<tr>
<td></td>
<td>The synchronization server must be declared as a Job server in One</td>
</tr>
<tr>
<td></td>
<td>Identity Manager. Use the following properties when you set up the Job</td>
</tr>
<tr>
<td></td>
<td>server.</td>
</tr>
</tbody>
</table>

Table 7: Additional properties for the Job server

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server function</td>
<td>SAP R/3 connector</td>
</tr>
<tr>
<td>Machine role</td>
<td>Server/Job server/SAP R/3</td>
</tr>
</tbody>
</table>

For more information, see Setting up the synchronization server on page 18.
Data | Explanation
--- | ---
One Identity Manager database connection data | • Database server
• Database
• SQL Server Login and password
• Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.

Remote connection server | To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with target system to do this. Sometimes direct access from the workstation on which the Synchronization Editor is installed is not possible, because of the firewall configuration, for example, or because the workstation does not fulfill the necessary hardware and software requirements. If direct access to the workstation is not possible, you can set up a remote connection.

The remote connection server and the workstation must be in the same Active Directory domain.

Remote connection server configuration:

• One Identity Manager Service is started
• RemoteConnectPlugin is installed
• SAP R/3 connector is installed

The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.

**TIP:** The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements). Use the synchronization as remote connection server at the same time, by simply installing the RemoteConnectPlugin as well.

For more detailed information about setting up a remote connection, see the *One Identity Manager Target System Synchronization Reference Guide*.

Additional information about setting up the synchronization project may be required depending on the configuration of the SAP R/3 system.

**Table 8: Information for setting up a synchronization project**

<table>
<thead>
<tr>
<th>Data</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP R/3</td>
<td>Name of the router that provides a network port for the SAP R/3 connector for</td>
</tr>
</tbody>
</table>
### Explanation

<table>
<thead>
<tr>
<th>Data</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>router</td>
<td>communicating with the application server.</td>
</tr>
<tr>
<td>SAP R/3 message server</td>
<td>Name of the message server with which the SAP R/3 connector communicates when logging in.</td>
</tr>
<tr>
<td>Login group</td>
<td>Name of the login group used by the SAP R/3 connector for logging in when communication is working over a message server within the SAP R/3 environment.</td>
</tr>
<tr>
<td>SNC host name</td>
<td>SNC name of the host for the secure network connection.</td>
</tr>
<tr>
<td>SNC Name</td>
<td>SCN name of the user account with which the SAP R/3 connector logs into the SAP R/3 system if a secure network connection is required. The SNC name must be entered using the same syntax as in the user account in SAP R/3.</td>
</tr>
<tr>
<td>SNC client API</td>
<td>API containing SNC encryption. Enter the file name and path of the synchronization server. Only file name is required if the file is in the default search path of the operating system. If encryption has been applied to the operating system, the file is located in the operating system directory and can be found via the standard search path. If a third-party product was used for encryption, the file can only be found if the installation directory of this product was added to the default search path (PATH variable).</td>
</tr>
</tbody>
</table>

**NOTE:** The following sequence describes how you configure a synchronization project if Synchronization Editor is both:

- executed In default mode, and
- started from the launchpad

If you execute the project wizard in expert mode or directly from Synchronization Editor, additional configuration settings can be made. Follow the project wizard instructions through these steps.

### To set up an initial synchronization project for an SAP client

1. Start the Launchpad and log on to the One Identity Manager database.

   **NOTE:** If synchronization is executed by an application server, connect the database through the application server.

2. Select **Target system type SAP R/3** and click **Start**.
   This starts the Synchronization Editor’s project wizard.

3. On the **System access** page, specify how One Identity Manager can access the target system.
If access is possible from the workstation on which you started Synchronization Editor, you do not need to make any settings.

If access is not possible from the workstation on which you started Synchronization Editor, you can set up a remote connection.

Enable the Connect using remote connection server option and select the server to be used for the connection under Job server.

4. Select a connection type on Connection type.

Table 9: Connector types

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP R/3 application server or SAP R/3 router</td>
<td>Specifies whether the connection is to be established through an application server or router</td>
</tr>
<tr>
<td>SAP R/3 message server</td>
<td>Specifies whether the connection is to be established through a message server</td>
</tr>
</tbody>
</table>

Enter the connection data for connection type "SAP R/3 application server or SAP R/3 router" on Connection data.

Table 10: System connection

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP R/3 host or router</td>
<td>Name of the application server or router used by the SAP R/3 connector for communication.</td>
</tr>
<tr>
<td>System number</td>
<td>Number of the SAP system</td>
</tr>
<tr>
<td>System ID</td>
<td>System ID of the SAP system The is used as the display name in One Identity Manager tools.</td>
</tr>
</tbody>
</table>

Enter the connection data for the "SAP R/3 message server" connection type on the Message server page.

Table 11: System connection

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP R/3 message server</td>
<td>Name of the message server used to establish the connection</td>
</tr>
<tr>
<td>Login group</td>
<td>Name of the login group used by the SAP R/3 connector for logging in</td>
</tr>
</tbody>
</table>
5. Enter the network settings on **Secure network communication**.

**Table 12: Network settings**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP R/3 router</td>
<td>Name of the router if the SAP R/3 connector communicates through a router</td>
</tr>
<tr>
<td>System number</td>
<td>Number of the SAP system</td>
</tr>
<tr>
<td>System ID</td>
<td>System ID of the SAP system This is used as the display name in One Identity Manager tools.</td>
</tr>
</tbody>
</table>

6. If you have enabled **SNC login** on **Secure connection, SNC connection configuration** opens. Enter the data required for logging into the target system using a secure network connection.

**Table 13: SNC system connection**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Number of the client to be synchronized. Enter the central system's client number if central user administration is to be synchronized.</td>
</tr>
<tr>
<td>SNC host name</td>
<td>SNC name of the host for the secure network connection.</td>
</tr>
<tr>
<td>SNC Name</td>
<td>SNC name of the user account used by the SAP R/3 connector to log in to the SAP R/3 system</td>
</tr>
<tr>
<td>SNC client API</td>
<td>API containing the SNC encryption</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select a security level for logging in to the SAP R/3 system.</td>
</tr>
<tr>
<td>Integrity protection</td>
<td>Encryption is enabled, but the highest available level is selected.</td>
</tr>
<tr>
<td>Highest available</td>
<td>Login language for logging the SAP R/3 connection into the SAP R/3 system. The language selected determines the language for captions for all SAP objects of this client. If you select &quot;EN&quot;, all texts from SAP groups, roles, profiles and start menus are synchronized in English.</td>
</tr>
</tbody>
</table>

7. Enter data for logging into the target system on **Login data**.

### Table 14: Login data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Number of the client to be synchronized. Enter the central system’s client number if central user administration is to be synchronized.</td>
</tr>
<tr>
<td>Login name</td>
<td>Name of the user account used by the SAP R/3 connector to log in to the SAP R/3 system. If you have enabled the option <strong>SNC login</strong> on the Secure connection page, enter the SNC name of this user account.</td>
</tr>
<tr>
<td>Login password</td>
<td>User account’s password that is used by the SAP R/3 connector to log in to the SAP R/3 system.</td>
</tr>
<tr>
<td>Login language</td>
<td>Login language for logging the SAP R/3 connection into the SAP R/3 system. The language selected determines the language for captions for all SAP objects of this client. If you select &quot;EN&quot;, all texts from SAP groups, roles, profiles and start menus are synchronized in English.</td>
</tr>
</tbody>
</table>

8. Supply additional information about synchronizing objects and properties on **Additional settings**. You can check the connection settings.

- In **Central user administration (CUA)**, specify whether the connection to a central user administration's central system should be established. In this case, set **CUA central system**.

- You can test the entered connection data in **Verify connection settings**. Click on **Verify project**.

  The system tries to connect to the server. If **CUA central system** is set, the given client is tested to see if it is the central system of a CUA.

  **NOTE:** There is no check on whether the supplied BAPI is installed.
9. Click **Next** on SAP **HCM settings**.
   This page is only needed for synchronizing additional personnel planning data in the SAP R/3 Structural Profiles Add-on Module.

10. Click **Next** on SAP **connector schema**.
    | **TIP:** You can enter a file with additional schema types on this page. The connector schema is extended by these custom schema types. You can also enter this data after saving the synchronization project. For more information, see Adding other schema types on page 39.

11. On the **One Identity Manager Connection** tab, test the data for connecting to the One Identity Manager database. The data is loaded from the connected database. Reenter the password.
    | **NOTE:** If you use an unencrypted One Identity Manager database and have not yet saved any synchronization projects to the database, you need to enter all connection data again. This page is not shown if a synchronization project already exists.

12. The wizard loads the target system schema. This may take a few minutes depending on the type of target system access and the size of the target system.

13. Select a project template on the **Select project template** page to use for setting up the synchronization configuration.

### Table 15: Standard project templates

<table>
<thead>
<tr>
<th><strong>Project template</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP R/3 (CUA subsystem)</td>
<td>Use this project template for initially setting up the synchronization project for a CUA’s child systems that belong to another SAP system than the central system.</td>
</tr>
<tr>
<td>SAP R/3 synchronization (base administration)</td>
<td>Use this project template for initially setting up the synchronization project for individual clients or a CUA’s central system.</td>
</tr>
</tbody>
</table>

| **NOTE:** A default project template ensures that all required information is added in One Identity Manager. This includes mappings, workflows and the synchronization base object. If you do not use a default project template you must declare the synchronization base object in One Identity Manager yourself. Use a default project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor. |
14. On the **Restrict target system access** page, you specify how system access should work. You have the following options:

**Table 16: Specify target system access**

<table>
<thead>
<tr>
<th>Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read-only access to target system.</td>
<td>Specifies whether a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database.</td>
</tr>
<tr>
<td></td>
<td>The synchronization workflow has the following characteristics:</td>
</tr>
<tr>
<td></td>
<td>* Synchronization is in the direction of <strong>One Identity Manager</strong>.</td>
</tr>
<tr>
<td></td>
<td>* Processing methods in the synchronization steps are only defined for synchronization in the direction of <strong>One Identity Manager</strong>.</td>
</tr>
<tr>
<td>Read/write access to target system.</td>
<td>Specifies whether a provisioning workflow is to be set up in addition to the synchronization workflow for the initial loading of the target system.</td>
</tr>
<tr>
<td>Provisioning available.</td>
<td>The provisioning workflow displays the following characteristics:</td>
</tr>
<tr>
<td></td>
<td>* Synchronization is in the direction of the <strong>Target system</strong>.</td>
</tr>
<tr>
<td></td>
<td>* Processing methods are only defined in the synchronization steps for synchronization in the direction of the <strong>Target system</strong>.</td>
</tr>
<tr>
<td></td>
<td>* Synchronization steps are only created for such schema classes whose schema types have write access.</td>
</tr>
</tbody>
</table>

This page is only shown if the project template **SAP® R/3® synchronization (basic administration)** was selected. If the **SAP® R/3® (child CUA system)** project template was selected, the **Read-only access to target system** option is automatically enabled.

15. Select the synchronization server to execute synchronization on the **Synchronization server** page.

If the synchronization server is not declared as a Job server in the One Identity Manager database yet, you can add a new Job server.

a. Click to add a new Job server.

b. Enter a name for the Job server and the full server name conforming to DNS syntax.

c. Click **OK**.
The synchronization server is declared as Job server for the target system in the One Identity Manager- database.

**NOTE:** After you save the synchronization project, ensure that this server is set up as a synchronization server.

16. To close the project wizard, click **Finish**.

This creates and allocates a default schedule for regular synchronization. Enable the schedule for regular synchronization.

The synchronization project is created, saved and enabled immediately.

**NOTE:** If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project automatically** option. In this case, save the synchronization project manually before closing the Synchronization Editor.

Disable this option, if you want to add your own schema types in this synchronization project.

**NOTE:** The connection data for the target system is saved in a variable set and can be modified under **Configuration | Variables** in Synchronization Editor.

**To configure the content of the synchronization log**

1. Open the synchronization project in the Synchronization Editor.
2. To configure the synchronization log for target system connection, select the category **Configuration | Target system**.
3. To configure the synchronization log for the database connection, select **Configuration | One Identity Manager connection**.
4. Select the **General** view and click **Configure**.
5. Select the **Synchronization log** view and set **Create synchronization log**.
6. Enable the data to be logged.

**NOTE:** Some content generates a particularly large volume of log data. The synchronization log should only contain data required for troubleshooting and other analyses.

7. Click **OK**.

**To synchronize on a regular basis**

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Configuration | Start up configurations**.
3. Select a start up configuration in the document view and click **Edit schedule**.
4. Edit the schedule properties.
5. To enable the schedule, click **Activate**.
6. Click **OK**.
To start initial synchronization manually

1. Open the synchronization project in the Synchronization Editor.
2. Select the category Configuration | Start up configurations.
3. Select a start up configuration in the document view and click Execute.
4. Confirm the security prompt with Yes.

**NOTE:**
Following a synchronization, employees are automatically created for the user accounts in the default installation. If an account definition for the client is not yet known at the time of synchronization, user accounts are linked with employees. However, account definitions are not assigned. The user accounts are therefore in a **Linked** state.

To manage the user accounts using account definitions, assign an account definition and a manage level to these user accounts.

**To select user accounts through account definitions**

1. Create an account definition.
2. Assign an account definition to the client.
3. Assign the account definition and manage level to user accounts in **linked** status.
   a. In Manager, select SAP R/3 | User accounts | Linked but not configured | <Client>.
   b. Select Assign account definition to linked accounts.

**Detailed information about this topic**

- One Identity Manager Target System Synchronization Reference Guide

**Related topics**

- Setting up the synchronization server on page 18
- Users and permissions for synchronizing with an SAP R/3 environment on page 14
- Displaying synchronization results on page 35
- Customizing synchronization configuration on page 35
- Speeding up synchronization with revision filtering on page 49
- Appendix: Default project templates for synchronizing an SAP R/3 environment on page 199
- Setting up account definitions on page 58
- Automatic assignment of employees to SAP user accounts on page 132
- Adding other schema types on page 39
Special features of synchronizing with a CUA central system

**NOTE:**

- Only child system roles and profiles that match the login language of the administrative user account for synchronization are mapped in One Identity Manager.
- Maintain all child system roles and profile in the target system in the language set as login language in the synchronization project for the central system in the system connection.

If a central user administration is connected to One Identity Manager, regular synchronization is only required with the central system. The synchronization configuration is created for the client labeled as central system. The CUA Application Link Enabling (ALE) distribution model is loaded during synchronization and tries to assign all clients, which are configured as child systems to the central system in One Identity Manager. All clients in the same SAP system as the central system are automatically added in One Identity Manager in the process and assigned to the central system (in **CUA central system**). All clients in another SAP system must already exist in One Identity Manager at this point in time.

If a text comparison of roles and profiles between child and central systems was executed the target system in the target system, the child system roles and profiles are taken into account by synchronization. These roles and profiles are assigned to the originating client in One Identity Manager.

Roles and profile are saved in USRSYSACTT with respect to language by text comparison of roles and profiles in the target system. Only roles and profile matching the login language of the administrative account for synchronization are read from the USRSYSACTT during synchronization with One Identity Manager. If single roles and profiles are not maintained in this language, they are not transferred to One Identity Manager. In order to map all roles and profiles from child systems in One Identity Manager, they must all be all maintained in the language specified as login language in the central system.

**To set up an initial synchronization project for central user administration**

1. Create synchronization projects the child systems, not in the same SAP system as the central system.

   Follow the steps described in Creating a synchronization project for initial synchronization of an SAP client on page 21. The following special features apply:
   
   a. In **Select project template** in the project wizard, select the project template "SAP R/3 (CUA subsystem)".
   
   b. The **Restrict target system access** page is not displayed. The target system is only loaded.
   
   c. Start synchronization manually to load the required data.

   All clients from the selected system and their license data are loaded.
NOTE: Do not synchronize using schedules. Re-synchronizing is only necessary if the active price lists for charging licenses were changed in the target system.

2. Repeat step 1 for all child system in other SAP subsystems.
3. Create a synchronization project for the central system.
   Follow the steps described in Creating a synchronization project for initial synchronization of an SAP client on page 21. The following special features apply:
   a. On the Additional settings page, enable Central User Administration (CUA) instance.
   b. On the Select project template page, select the "SAP R/3 synchronization (base administration)" project template.
   c. Configure the scheduled synchronization,
4. Start central system synchronization, after all child systems have been loaded in the SAP database from One Identity Manager subsystems.

Related topics
- General master data for an SAP client on page 103
- Excluding a child system from synchronization on page 33

Excluding a child system from synchronization

Certain administrative task in SAP R/3 required that the child system is temporarily excluded from the central user administration. If these child systems are synchronized during this period, the SAP roles and SAP profile of the temporarily excluded child system are marked as outstanding or deleted in the One Identity Manager database. To prevent this, remove the child system from the synchronization scope.

SAP roles and profiles are removed from the synchronization scope by deleting the ALE model name in the client. The client properties are synchronized anyway. To ensure that the ALE model name is not reintroduced, disable the rule for mapping this schema property.

To exclude a child system from synchronization
1. Select SAP R/3 | Clients.
2. Select the child system in the result list. Select Change master data.
3. Delete the entry in ALE model name.
4. Save the changes.
5. Open the synchronization project in the Synchronization Editor.
6. Select the category Workflows.
7. Select the workflow to use for synchronizing the central system in the navigation view.
10. Select "ALEModelName_ALEModelName" in Excluded rules.
11. Click OK.
12. Save the changes.

**NOTE:** Unsuccessful database operations for assigning SAP roles and profiles to user account that originate from the temporarily excluded child system are logged depending on the setting in the synchronization log. You can ignore these messages. Once the child system is available again, the memberships are handled properly.

You must reactivate synchronization of the child system's SAP role and profiles the moment it becomes part of the central user administration again.

**To re-include a child system in synchronization**

1. Select SAP R/3 | Clients.
2. Select the child system in the result list. Select **Change master data**.
3. Enter the ALE model name of the central system's CUA in **ALE model name**.
   
   The child system is only synchronized if the same ALE model named is entered in the central system and the child system.
4. Save the changes.
5. Open the synchronization project in the Synchronization Editor.
6. Select the category **Workflows**.
7. Select the workflow in the navigation, to use for synchronizing the central system (default is "Initial Synchronization").
10. Deselect "ALEModelName_ALEModelName" in Excluded rules.
11. Click OK.
12. Save the changes.

For more information about editing synchronization steps, see One Identity Manager Target System Synchronization Reference Guide.

**Related topics**

- [General master data for an SAP client](#) on page 103
Displaying synchronization results

Synchronization results are summarized in the synchronization log. You can specify the extent of the synchronization log for each system connection individually. One Identity Manager provides several reports in which the synchronization results are organized under different criteria.

To display a synchronization log

1. Open the synchronization project in the Synchronization Editor.
2. Select Logs.
3. Click in the navigation view toolbar.
   Logs for all completed synchronization runs are displayed in the navigation view.
4. Select a log by double-clicking on it.
   An analysis of the synchronization is shown as a report. You can save the report.

To display a provisioning log.

1. Open the synchronization project in the Synchronization Editor.
2. Select Logs.
3. Click in the navigation view toolbar.
   Logs for all completed provisioning processes are displayed in the navigation view.
4. Select a log by double-clicking on it.
   An analysis of the provisioning is shown as a report. You can save the report.

The log is marked in color in the navigation view. This mark shows you the execution status of the synchronization/provisioning.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

- In Designer, enable the DPR | Journal | LifeTime configuration parameter and enter the maximum retention period.

Customizing synchronization configuration

You have set up a synchronization project using the Synchronization Editor for initial synchronization of an SAP client. You can use this synchronization project to load SAP objects into the One Identity Manager database. If you manage user accounts and their authorizations with One Identity Manager, changes are provisioned in the SAP environment.
You must customize the synchronization configuration in order to compare the SAP R/3 database with the regularly and to synchronize changes.

- To use One Identity Manager as the master system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- To specify which SAP objects and database object are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.
- You can use variables to create generally applicable synchronization configurations that contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes, or processing methods, for example.
- Use variables to set up a synchronization project which can be used for several different clients. Store a connection parameter as a variable for logging in to the clients.
- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.
- Add your own schema types if you want to synchronize data, which does not have schema types in the connector schema.

**IMPORTANT:** As long as synchronization is running, you must not start another synchronization for the same target system. This applies especially, if the same synchronization objects would be processed.

- If another synchronization is started with the same start up configuration, this process is stop and is assigned the **Frozen** execution status. An error message is written to the One Identity Manager Service log file.
- If another synchronization is started with another start up configuration, that addresses same target system, it may lead to synchronization error or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration.
  - Use the schedule to ensure that the start up configurations are executed in sequence.
  - Group start up configurations with the same start up behavior.

For more detailed information about configuring synchronization, see the One Identity Manager Target System Synchronization Reference Guide.

**Detailed information about this topic**

- How to configure synchronization in the SAP R/3 environment on page 37
- Configuring synchronization of different clients on page 37
- Updating schemas on page 38
- Adding other schema types on page 39
How to configure synchronization in the SAP R/3 environment

The synchronization project for initial synchronization provides a workflow for initial loading of target system objects (initial synchronization) and one for provisioning object modifications from the One Identity Manager database to the target system (provisioning). To use One Identity Manager as the master system during synchronization, you also require a workflow with synchronization in the direction of the Target system.

To create a synchronization configuration for synchronizing SAP R/3

1. Open the synchronization project in the Synchronization Editor.
2. Check whether existing mappings can be used for synchronizing the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard. Creates a workflow with Target system as its synchronization direction.
4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Related topics

- Configuring synchronization of different clients on page 37

Configuring synchronization of different clients

Prerequisites

- The target system schema of both clients are identical.
- All virtual schema properties used in the mapping must exist in the extended schema of both clients.

To customize a synchronization project for synchronizing another client

1. Prepare a user account with sufficient permissions for synchronizing in the other client.
2. Open the synchronization project in the Synchronization Editor.
3. Create a new base object for the other clients. Use the wizards to attach a base object.
In the wizard, select the SAP connector and declare the connection parameters. The connection parameters are saved in a special variable set. A start up configuration is created, which uses the newly created variable set.

4. Change other elements of the synchronization configuration as required.
5. Save the changes.
6. Run a consistency check.

Related topics

- How to configure synchronization in the SAP R/3 environment on page 37

Updating schemas

All the schema data (schema types and schema properties) of the target system schema and the One Identity Manager schema are available when you are editing a synchronization project. Only a part of this data is really needed for configuring synchronization. If a synchronization project is finished, the schema is compressed to remove unnecessary data from the synchronization project. This can speed up loading the synchronization project. Deleted schema data can be added to the synchronization configuration again at a later point.

If the target system schema or the One Identity Manager schema has changed, these changes must also be added to the synchronization configuration. Then the changes can be added to the schema property mapping.

To include schema data that have been deleted through compressing and schema modifications in the synchronization project, update each schema in the synchronization project. This may be necessary if:

- A schema was changed by:
  - Changes to a target system schema
  - Customizations to the One Identity Manager schema
  - A One Identity Manager update migration
- A schema in the synchronization project was shrunk by:
  - enabling the synchronization project
  - saving the synchronization project for the first time
  - compressing a schema

To update a system connection schema

1. Open the synchronization project in the Synchronization Editor.
2. Select Configuration | Target system.
   - OR -
Select Configuration | One Identity Manager Connection.

3. Select the view General and click Update schema.
4. Confirm the security prompt with Yes.
   This reloads the schema data.

To edit a mapping

1. Open the synchronization project in the Synchronization Editor.
2. Select the category Mappings.
3. Select a mapping in the navigation view.
   Opens the Mapping Editor. For more detailed information about mappings, see the One Identity Manager Target System Synchronization Reference Guide.

| NOTE: | The synchronization is deactivated if the schema of an activated synchronization project is updated. Reactivate the synchronization project to synchronize.

Adding other schema types

Add your own schema types if you want to synchronize data, which does not have schema types in the connector schema. You can let your own schema types be added when setting up the initial synchronization project with the project wizard. However, you can also add them after saving the synchronization project. This method is described here.

You can obtain an overview of which schema types are defined in the connector schema in the Synchronization Editor target system browser.

| IMPORTANT: | Both used and unused schema types are displayed in the Target System Browser. If the synchronization project is set, unused system types are deleted from the schema. Then they are longer appear in the Target System Browser.
   Check the schema type list before you enable the synchronization project.

To start the Target System Browser

1. Open the synchronization project in the Synchronization Editor.
2. Select Configuration | Target system.
3. Select the General view and click Browse....
   This opens the Target System Browser. You will see all the schema types used in this synchronization project in the upper pane of the Schema types view. The lower pane contains the list of unused schema types

To extend the connector schema with your own schema types

1. Find which out schema types you require.
2. Create a schema extension file. Save this file and keep the file name and path at the
For more information, see Creating a schema extension file on page 40.

3. Open the synchronization project in the Synchronization Editor.

4. Select Configuration | Target system.

5. Click Edit connection.
   This starts the system connection wizard.

6. Verify the data.

7. Enter the name and path of your schema extension file on the SAP connector schema page.
   a. To check the schema extensions file for logical errors, click Test file.
      All defined schema types are listed.
   b. Click Next.

8. Click Finish to end the system connection wizard.

9. Select the view General and click Update schema.

10. Confirm the security prompt with Yes.
    The schema types, including your new schema types, are loaded.

11. Open the Target System Browser and check whether the schema types have been added.
    The schema types are displayed in the list of used schema types.

12. Select the category Mapping and create mappings for the your new schema types.
    Take note of whether these are read-only or whether read/write access is permitted.
    For detailed information about setting up mapping and schema classes, see the One Identity Manager Target System Synchronization Reference Guide.

13. Select the Workflows category and edit the workflows. Create additional synchronization steps for the new mappings. Take note of whether the schema types are read-only or whether read/write access is permitted.
    For detailed information about setting up synchronization steps, see the One Identity Manager Target System Synchronization Reference Guide.

14. Save the changes.

15. Run a consistency check.

16. Activate the synchronization project.

Creating a schema extension file

Define all the schema types you want to use to extend the connector schema in the schema extension file. The schema extension file is an XML file with a structure identical to the connector schema. It describes the definitions for table queries and BAPI calls for the new
schema types. If a new schema type has the same name as an already existing schema type, the extension is ignored.

The file is divided into three main sections:

- Table section
- Functions section
- Schema types section

Basically, tables and functions required to access data for defined schema types, must be declared first. Then you can define new schema types in the schema types section. Use 'functions and tables in different schema type definitions in this case. A schema type definition must contain at least one call for an object list.

**Schema Extension File Structure**

```xml
<?xml version="1.0" encoding="utf-8" ?>
<SAP>
  <Tables>...
  </Tables>
  <Functions>...
  </Functions>
  <SAPExtendedSchematypes>...
  </SAPExtendedSchematypes>
</SAP>
```

**Predefined variables**

You can use variables in the table and function sections. These can be all the system variables known to the SAP module RFC_READ_TABLE.

**Table 17: System variable examples**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sy-langu</td>
<td>Currently selected login language.</td>
</tr>
<tr>
<td>sy-datum</td>
<td>Current date.</td>
</tr>
<tr>
<td>sy-mandant</td>
<td>Current client.</td>
</tr>
</tbody>
</table>

You can also use variables known to the SAP R/3 connector, for example, from the process parameter definition.
Table 18: Predefined SAP R/3 connector variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Value$</td>
<td>Input parameter for the One Identity Manager Service call.</td>
</tr>
<tr>
<td>$Mandt$</td>
<td>Current client's number.</td>
</tr>
<tr>
<td>$Date$</td>
<td>Current date.</td>
</tr>
</tbody>
</table>

Detailed information about this topic

- Defining tables on page 42
- Defining functions on page 45
- Defining schema types on page 46
- Appendix: Example of a schema extension file on page 206

Defining tables

In the section for tables (Tables), you can select tables and columns required for accessing the data for the schema types that will be defined. The SAP R/3 connector requires a definition for each table to load the slim object list. To do this, you define exactly those columns the SAP R/3 connector required when it loaded the synchronization objects. All columns in the table are loaded when single objects are accessed.

Table 19: Table definition

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition</td>
<td>Symbolic name for using the definition.</td>
</tr>
<tr>
<td>TableName</td>
<td>Name of the table in the SAP database.</td>
</tr>
<tr>
<td>Key</td>
<td>Key term for formatting the distinguished name. Multiple values can be entered in a comma delimited list.</td>
</tr>
<tr>
<td>X500</td>
<td>Abbreviation for the key term in the attribute key. Multiple values can be entered in a comma delimited list.</td>
</tr>
<tr>
<td>SQL</td>
<td>Limiting WHERE clause.</td>
</tr>
</tbody>
</table>
NOTE: There are a number of restrictions for parsing SQL operators in the SAP R/3 system. Take the following rules into account to ensure correctness:

- The column name must be in front of the operator in a comparison and the comparison value after it (for example, BEGDA LT sy-datum).
- The comparison operators "<" and ">" cause parsing errors in XML. Use the operators LT and GT instead. For more information, see Permitted operators in the SQLattribute on page 43.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distinct</td>
<td>Counts the columns that the Distinct filter applies to (as comma delimited list).</td>
</tr>
<tr>
<td>Load</td>
<td>Columns to load when the object list is loaded. These columns can be for can be used to format the schema type's display name (DisplayPattern) as revision counters, for example, or as input parameters in a function, If the object list is loaded from a table but single objects from a function, all the columns used within the synchronization project mapping must be given here.</td>
</tr>
</tbody>
</table>

IMPORTANT: Each column, which must be additionally loaded when the object list is loaded, creates extra load for One Identity Manager. This can make synchronization much slower if there is a lot of data. Only enter columns that you really need for further object processing.

No data is required for single object access.

Advice

- Several table definitions with different symbolic names can be defined that refer to the same table in the SAP database.
- Key columns are always loaded. They should not, therefore, be given in the Load attribute.
- The Load attribute only works when loading the object list. All columns of the table are always loaded for single object access.
- The following operators are permitted in the WHERE clause:

Table 20: Permitted operators in the SQLattribute

<table>
<thead>
<tr>
<th>Operator</th>
<th>Function/example</th>
</tr>
</thead>
<tbody>
<tr>
<td>EQ</td>
<td>=</td>
</tr>
<tr>
<td>Operator</td>
<td>Function/example</td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
</tr>
<tr>
<td>NE</td>
<td>&lt;&gt;</td>
</tr>
<tr>
<td>GT</td>
<td>&gt;</td>
</tr>
<tr>
<td>LT</td>
<td>&lt;</td>
</tr>
<tr>
<td>GE</td>
<td>&gt;=</td>
</tr>
<tr>
<td>LE</td>
<td>&lt;=</td>
</tr>
</tbody>
</table>

**Example:**

```xml
<Tables>
  <TABLE Definition = "HRP1001-Table" TableName="HRP1001"
Key="OTJID,SUBTY,BEGDA,ENDDA" X500="CN,OU,OU,OU" SQL="MANDT = sy-mandt"
Load="VARYF" Distinct="OTJID,SUBTY,VARYF" />
  <TABLE Definition = "HRP1000-Table" TableName="HRP1000"
Key="OTJID,LANGU,BEGDA,ENDDA" X500="CN,OU,OU,OU" SQL="MANDT = sy-mandt" Load=""
Distinct="OTJID" />
  <TABLE Definition = "RSECUSERAUTH-SingleUser" TableName="RSECUSERAUTH" Key="AUTH"
X500="CN" SQL="UNAME = '$BNAME$'" Load="" >
    <Mapping>
      <Data ParameterName = "$BNAME$" PropertyName = "USERNAME" />
    </Mapping>
  </TABLE>
</Tables>
```
Defining functions

In the section for functions (Functions), you can describe the interfaces to BAPI functions required for accessing the data for the schema types, which will be defined.

Table 21: Function definition

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition</td>
<td>Symbolic name for using the definition.</td>
</tr>
<tr>
<td>FunctionName</td>
<td>Function name in the SAP R/3 system.</td>
</tr>
<tr>
<td>OutStructure</td>
<td>Name of an SAP structure given as a return value. (Optional)</td>
</tr>
<tr>
<td>Key</td>
<td>Key term for formatting the distinguished name. Multiple values can be entered in a comma delimited list.</td>
</tr>
<tr>
<td>X500</td>
<td>Abbreviation for the key term in the attribute Key. Multiple values can be entered in a comma delimited list.</td>
</tr>
</tbody>
</table>

In the optional mapping block, you define how the values are passed to the function call parameters. To do this, an object list must be created before the function call. The parameters for the function call can be filled from this object list's properties. In the example below, BNAME is a property, which is determined from the object list of the table USR02.

Predefined variables can be passed to the parameters. For more information, see Creating a schema extension file on page 40. Apart from that, it is possible to pass a fixed value to a function parameter. The following notation is provided for this.

Example:

```xml
<Data ParameterName = "<Name>" PropertyName = "VALUE=<fixed value>" />

Example:

<Tables>
  <TABLE Definition = "USR02-Table" TableName="USR02" Key="BNAME" X500="CN"
    SQL="MANDT = '$MANDT$'" Load="" />
</Tables>

<Functions>
  <Function Definition = "USER GET" FunctionName="BAPI_USER_GET_DETAIL"
    OutStructure = "" Key ="USERNAME" X500 ="CN">
    <Mapping>
      <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
    </Mapping>
  </Function>
</Functions>
```
Defining schema types

In the section for schema types (SAPExtendedSchematypes), you can define schema types that exist in the SAP schema and can be used to extend the connector schema. The identifier given in the attribute Name is used as the name. This identifier must be unique in the extended connector schema.

Table 22: Schema type definition

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bem</td>
<td>Internal description</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the schema type in the extended connector schema.</td>
</tr>
<tr>
<td>DisplayPattern</td>
<td>Definition of a display pattern for displaying objects in the Synchronization Editor (for example, in the target system browser or defining schema classes). (Optional) Only columns that are loaded in the table definition (attribute Key or Load) can be used.</td>
</tr>
<tr>
<td>RevisionProperty</td>
<td>Name of a property contain the revision counter. (Optional)</td>
</tr>
<tr>
<td>ListObjectsDefinition</td>
<td>Function or table definition for calling an object list.</td>
</tr>
<tr>
<td>ReadObjectDefinition</td>
<td>Function or table definition for calling a single object.</td>
</tr>
<tr>
<td>WriteObjectDefinition</td>
<td>Function definition for writing an object. (Optional)</td>
</tr>
<tr>
<td>DeleteObjectDefinition</td>
<td>Function definition for deleting an object. (Optional)</td>
</tr>
<tr>
<td>ParentType</td>
<td>Context of the schema type. (Optional)</td>
</tr>
</tbody>
</table>

By default, the schema types are client-related (ParentType="SAPMANDANT"). If the new schema type is valid in all SAP R/3 system clients, enter ParentType with the value "SAPSYSTEM".

If this attribute is not defined, the schema type is client-related.

A schema type definition must contain at least one object list call (attribute ListObjectsDefinition). In this case, you can enter a table or a function definition. To call a single object (attribute ReadObjectDefinition), the object list must have been loaded.

Related topics

- Appendix: Example of a schema extension file on page 206
previously. The list call and single object call can refer to different tables, however the key columns for identifying single objects must either have the same name or have been mapped in the table definition for the single object call. In the example below, the single objects from table RSECUSERAUTH are determined for an object from the table USR02. The key columns for identifying the objects are USR02.BNAME and RSECUSERAUTH.UNAME. The columns have different names and are therefore mapped using the parameter $BNAME$.

If is possible to define a Properties block for declaring any number of other object properties and the types of access to them. One single property is defined by the Property tag, which can have the following attributes.

Table 23: Property definition

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the property. It must be unique within the schema type.</td>
</tr>
<tr>
<td>Description</td>
<td>Property description.</td>
</tr>
<tr>
<td>ListFunction</td>
<td>Function or table for calling all values.</td>
</tr>
<tr>
<td>AddFunction</td>
<td>Function for adding a value. (Optional)</td>
</tr>
<tr>
<td>DelFunction</td>
<td>Function for deleting a value. (Optional)</td>
</tr>
<tr>
<td>ReplaceFunction</td>
<td>Replaces the entire contents of the property. (Optional)</td>
</tr>
<tr>
<td>IsMultivalued</td>
<td>Specifies whether the property has multiple values. (Optional)</td>
</tr>
</tbody>
</table>

If this attribute is not defined, the property does not have multiple values.

Example:

```xml
<Tables>
  <TABLE Definition = "USR04-Table" TableName="USR04" Key="BNAME,MANDT"
X500="CN,OU" SQL="MANDT = sy-mandt" Load="" />
  <TABLE Definition = "USR02-Table" TableName="USR02" Key="BNAME" X500="CN"
SQL="MANDT = sy-mandt" Load="MANDT,TRDAT" />
  <TABLE Definition = "RSECUSERAUTH-SingleUser" TableName="RSECUSERAUTH" Key="AUTH"
X500="CN" SQL="UNAME = '$BNAME$'" Load="" >
    <Mapping>
      <Data ParameterName = "$BNAME$" PropertyName = "BNAME" />
    </Mapping>
  </TABLE>
</Tables>

<Functions>
  <Function Definition = "USER GET" FunctionName="BAPI_USER_GET_DETAIL"
OutStructure = "" Key ="USERNAME" X500 ="CN">
```
<Mapping>
  <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
</Mapping>

</Function>

<Function Definition = "USER SET" FunctionName="BAPI_USER_CHANGE" OutStructure =""
  Key ="USERNAME" X500 ="CN">
  <Mapping>
    <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
  </Mapping>
</Function>

<Function Definition = "USER DEL" FunctionName="BAPI_USER_DELETE" OutStructure =""
  Key ="USERNAME" X500 ="CN">
  <Mapping>
    <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
  </Mapping>
</Function>

<Function Definition = "USER PROFILE SET" FunctionName="BAPI_USER_PROFILES_ASSIGN" OutStructure =""
  Key ="USERNAME" X500 ="CN">
  <Mapping>
    <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
    <Data ParameterName = "BAPIPROF~BAPIPROF" PropertyName = "$Value$" />
  </Mapping>
</Function>

<Function Definition = "BWProfileDelFkt" FunctionName="/VIAENET/SAPHR_RSECUSERAUT_DEL"
  OutStructure =""
  Key ="ZUSRNAME,ZHIER" X500 ="CN,OU">
  <Mapping>
    <Data ParameterName = "ZUSRNAME" PropertyName = "BNAME" />
    <Data ParameterName = "ZHIER" PropertyName = "$VALUE$" />
  </Mapping>
</Function>

<Function Definition = "BWProfileAddFkt" FunctionName="/VIAENET/SAPHR_RSECUSERAUT_ADD"
  OutStructure =""
  Key ="ZUSRNAME,ZHIER" X500 ="CN,OU">
  <Mapping>
    <Data ParameterName = "ZUSRNAME" PropertyName = "BNAME" />
    <Data ParameterName = "ZHIER" PropertyName = "$VALUE$" />
  </Mapping>
</Function>
Explanation:

The list of schema type objects UserFunctionTable is created by using the table USR02. Reading, writing, and deleting is done with USER-BAPI functions, which each have been declared as a Function.

The schema type has a properties block. Two properties are defined here that are neither returned through the list call’s table definition nor through the single object call’s function definition. A multi-value property SAPBWP is defined, whose value is taken from the table RSECUSERAUTH. The single objects are identified by the columns USR02.BNAME and RSECUSERAUTH.UNAME. BAPI calls, which are defined as functions, are used for inserting and deleting values.

The property Userprofile is an example of a multi-value property, which has values read from a table (USR04) and a Replace function. Therefore, all values that need to remain in the property must always be given when changes are made. The write function is the original USER-BAPI function for setting profiles in the user (function definition for BAPI_ USER_PROFILES_ASSIGN). Single objects are identified using the columns USR02.BNAME and USR04.BNAME. There is no mapping required for the table definition because the key columns have the same name.

Speeding up synchronization with revision filtering

When you start synchronization, all synchronization objects are loaded. Some of these objects have not be modified since the last synchronization and, therefore, must not be
processed. Synchronization is accelerated by only loading those object pairs that have changed since the last synchronization. One Identity Manager uses revision filtering to accelerate synchronization.

SAP R/3 supports revision filtering. The SAP objects' date of last change is used as revision counter. Each synchronization saves its last execution date as a revision in the One Identity Manager database (table DPRRevisionStore, column Value). This value is used as a comparison for revision filtering when the same workflow is synchronized the next time. When this workflow is synchronized the next time, the SAP objects' change date is compared with the revision saved in the One Identity Manager database. Only those objects that have been changed since this date are loaded from the target system.

**NOTE:** SAP roles are given the last date the role was generated in the target system. Only SAP roles that have be regenerated since the last synchronization are updated in the database on synchronization with revision filtering.

The revision is found at start of synchronization. Objects changed after this point are included with the next synchronization.

Revision filtering can be applied to workflows and start up configuration.

**To permit revision filtering on a workflow**
- Open the synchronization project in the Synchronization Editor.
- Edit the workflow properties. Select the entry **Use revision filter** from **Revision filtering**.

**To permit revision filtering for a start up configuration**
- Open the synchronization project in the Synchronization Editor.
- Edit the start up configuration properties. Select the entry **Use revision filter** from **Revision filtering**.

**Detailed information about this topic**
- One Identity Manager Target System Synchronization Reference Guide

**Synchronizing collective roles**

Only directly assigned single and collective roles are mapped in SAPUserInSAPRole. Assignments of single roles to collective roles are mapped in SAPCollectionRPG. You can establish which single roles are indirectly assigned to a user account through both tables.

By default, the following applies to inheritance of single roles by user accounts: If a single role is assigned to a user account and the single role is part of a collective role, which is also assigned to the user account the single role is not inherited by the user account as well. This removes membership of user accounts in single roles when group memberships are provisioned in SAP R/3. This membership is deleted from the One Identity Manager.
database by the next synchronization or marked as outstanding, depending on the synchronization's configuration.

To prevent memberships being removed from single roles when single roles are part of collective roles

- Set "TargetSystem\SAP\KeepRedundantProfiles" in the Designer.

Restricting synchronization objects using user permissions

One Identity Manager offers the ability to restrict user account and groups for synchronization by using user permissions. In this case, the only user accounts and groups that are synchronized are those used by the SAP R/3 connector to log into the target system. All other groups and user accounts are filtered out of the user lists and the groups list of the function module "/VIAENET/U". If only a small part of the user account in the SAP R/3 environment should be synchronized with the One Identity Manager then the synchronization can be accelerated with this method.

Prerequisites

- The user account used by the SAP R/3 connector to log into the target system is assigned exactly those groups in the SAP R/3 authorization object S_USER_GRP, characteristic CLASS, that should be synchronized.
- There are user accounts that one of these groups is assigned to in the SAP R/3 environment as user group for testing authorization (in the login data).

During synchronization, the groups are loaded into the One Identity Manager database that the user account used by the SAP R/3 connector to log into the target system has access to in the authorization object SUSER_GRP. All user accounts that are assigned one of these groups as user group for authorization testing, are also synchronized. All other groups and user accounts are handled as non-existent objects in the target system during synchronization.

Post-processing outstanding objects

Objects, which do not exist in the target system, can be marked as outstanding in One Identity Manager by synchronizing. This prevents objects being deleted because of an incorrect data situation or an incorrect synchronization configuration.

Outstanding objects
- Cannot be edited in One Identity Manager.
- Are ignored by subsequent synchronization.
- Are ignored by inheritance calculations.

This means, all memberships and assignments remain intact until the outstanding objects have been processed.

Start target system synchronization to do this.

**To post-process outstanding objects**

1. In Manager, select the **SAP R/3 | Target system synchronization: SAP R/3** category.
   
   All tables assigned to the target system type **SAP R/3** as synchronization tables are displayed in the navigation view.

2. On the **Target system synchronization** form, in the **Table / object** column, open the node of the table for which you want to post-process outstanding objects.
   
   All objects that are marked as outstanding are shown. The **Last log entry** and **Last method run** columns display the time at which the last entry was made in the synchronization log and which processing method was executed. The **No log available** entry can mean the following:
   - The synchronization log has already been deleted.
   - OR -
   - An assignment from a member list has been deleted in the target system.
     
     The base object of the assignment has been updated during the synchronization. A corresponding entry appears in the synchronization log. The entry in the assignment table is marked as outstanding, but there is no entry in the synchronization log.

3. Select the objects you want to rework. Multi-select is possible.

4. Click one of the following icons in the form toolbar to execute the respective method.

   TIP:

   **To display object properties of an outstanding object**
   
   a. Select the object on the target system synchronization form.
   
   b. Open the context menu and click **Show object**.
Table 24: Methods for handling outstanding objects

<table>
<thead>
<tr>
<th>Icon</th>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Delete</td>
<td>The object is immediately deleted in the One Identity Manager database. Deferred deletion is not taken into account. The Outstanding label is removed for the object. Indirect memberships cannot be deleted.</td>
</tr>
</tbody>
</table>
| ![Icon] | Publish | The object is added in the target system. The Outstanding label is removed for the object. The method triggers the HandleOutstanding event. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites:  
  - The table containing the object can be published.  
  - The target system connector has write access to the target system. |
| ![Icon] | Reset | The Outstanding label is removed for the object. |

5. Confirm the security prompt with Yes.

**NOTE:** By default, the selected objects are processed in parallel, which speeds up execution of the selected method. If an error occurs during processing, the action is stopped and all changes are discarded.

Bulk processing of objects must be disabled if errors are to be localized, which means the objects are processed sequentially. Failed objects are named in the error message. All changes that were made up until the error occurred are saved.

To disable bulk processing

- Deactivate ![Deactivate] in the form toolbar.

You must customize synchronization to synchronize custom tables.

**To add custom tables to the target system synchronization**

1. In Manager, select SAP R/3 | Basic configuration data | Target system types.
2. In the result list, select the target system type SAP R/3.
3. Select Assign synchronization tables.
4. Assign custom tables whose outstanding objects you want to handle in Add assignments.
5. Save the changes.
6. Select Configure tables for publishing.
7. Select custom tables whose outstanding objects can be published in the target system.
system and set **Publishable**.

8. Save the changes.

**NOTE:** The target system connector must have write access to the target system in order to publish outstanding objects that are being post-processed. That means, the option **Connection is read only** must no be set for the target system connection.

### Configuring the provisioning of memberships

Memberships, for example, user accounts in groups, are saved in assignment tables in the One Identity Manager database. During provisioning of modified memberships, changes made in the target system will probably be overwritten. This behavior can occur under the following conditions:

- Memberships are saved in the target system as an object property in list form (Example: List of role assignments in the AGR_NAME property of the SAP R/3 user).
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

If a membership in One Identity Manager changes, the complete list of members is transferred to the target system by default. Memberships, previously added to the target system are removed by this; previously deleted memberships are added again.

To prevent this, provisioning can be configured such that only the modified membership is provisioned in the target system. The corresponding behavior is configured separately for each assignment table.

**To allow separate provisioning of memberships**

1. In Manager, select **SAP R/3 | Basic configuration data | Target system types**.
2. Select **SAP R/3** in the result list.
3. Select **Configure tables for publishing**.
4. Select the assignment tables for which you want to allow separate provisioning. Multi-select is possible.
   - This option can only be enabled for assignment tables that have a base table with XDateSubItem or CCC_XDateSubItem column.
   - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically.
5. Click **Enable merging**.
6. Save the changes.

For each assignment table labeled like this, the changes made in One Identity Manager are saved in a separate table. During modification provisioning, the members list in the target
system is compared to the entries in this table. This means that only modified memberships are provisioned and the members list does not get entirely overwritten.

**NOTE:** The complete members list is updated by synchronization. During this process, objects with changes but incomplete provisioning are not handled. These objects are logged in the synchronization log.

For more detailed information about provisioning memberships, see the One Identity Manager Target System Synchronization Reference Guide.

**NOTE:** Changes to user account memberships in single role are *always* provisioned individually. Therefore, single provisioning cannot be configured for the table SAPUserInSAPRole.

### Help for the analysis of synchronization issues

You can generate a report for analyzing problems which occur during synchronization, for example, insufficient performance. The report contains information such as:

- Consistency check results
- Revision filter settings
- Scope applied
- Analysis of the synchronization buffer
- Object access times in the One Identity Manager database and in the target system

**To generate a synchronization analysis report**

1. Open the synchronization project in the Synchronization Editor.
2. Select the menu **Help | Generate synchronization analysis report** and answer the security prompt with **Yes**.
   
   The report may take a few minutes to generate. It is displayed in a separate window.
3. Print the report or save it in one of the available output formats.

### Disabling synchronization

Regular synchronization cannot be started until the synchronization project and the schedule are active.
To prevent regular synchronization

1. Open the synchronization project in the Synchronization Editor.
2. Select the start up configuration and deactivate the configured schedule.

   Now you can only start synchronization manually.

An activated synchronization project can only be edited to a limited extend. The schema in the synchronization project must be updated if schema modifications are required. The synchronization project is deactivated in this case and can be edited again.

Furthermore, the synchronization project must be deactivated if synchronization should not be started by any means (not even manually).

To deactivate the synchronization project

1. Open the synchronization project in the Synchronization Editor.
2. Select General on the start page.
3. Click Deactivate project.

Detailed information about this topic

- Creating a synchronization project for initial synchronization of an SAP client on page 21
Basic data for managing an SAP R/3 environment

The following basic data is relevant for managing an SAP R/3 environment in One Identity Manager.

- **Configuration parameter**
  Use configuration parameters to configure the behavior of the system's basic settings. One Identity Manager provides default settings for different configuration parameters. Check the configuration parameters and modify them as necessary to suit your requirements.

  Configuration parameters are defined in the One Identity Manager modules. Each One Identity Manager module can also install configuration parameters. You can find an overview of all configuration parameters in **Base data | General | Configuration parameters** in Designer.

  For more information, see Appendix: Configuration parameters for managing an SAP R/3 environment on page 194.

- **Account definitions**
  One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. You can create account definitions for every target system. If an employee does not yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

  For more information, see Setting up account definitions on page 58.

- **Password policies**
  One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

  Predefined password policies are supplied with the default installation that you can user or customize if required. You can also define your own password policies.

  For more information, see Password policies for SAP user accounts on page 81.
- Initial password for new user accounts
  You have the different options for issuing an initial password for user accounts. The central password of the assigned employee can be aligned with the user account password, a predefined, fixed password can be used or a randomly generated initial password can be issued.
  For more information, see Initial password for new SAP user accounts on page 91.
- Email notifications about login data
  When a new user account is created, the login data are send to a specified recipient. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages.
  For more information, see Email notifications about login data on page 93.
- Login Languages
  User accounts can be assigned a default login language. Login languages can be loaded into the One Identity Manager database through synchronization.
  For more information, see Login languages on page 79.
- Target system types
  Target system types are required for configuring target system comparisons. Tables containing outstanding objects are maintained on target system types.
  For more information, see Post-processing outstanding objects on page 51.
- Server
  In order to handle SAP R/3-specific processes in One Identity Manager, the synchronization server and its server functions must be declared.
  For more information, see Editing a server on page 94.
- Target system managers
  A default application role exists for the target system manager in One Identity Manager. Assign the employees who are authorized to edit all clients in One Identity Manager to this application role.
  Define additional application roles if you want to limit the edit permissions for target system managers to individual clients. ns for target system managers to individual farms. SharePoint The application roles must be added under the default application role.
  For more information, see Target system managers on page 99.

### Setting up account definitions

One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. You can create account definitions for every target system. If an employee does not yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.
The data for the user accounts in the respective target system comes from the basic employee data. The employee must own a central SAP user account. The assignment of the IT operating data to the employee’s user account is controlled through the primary assignment of the employee to a location, a department, a cost center, or a business role (template processing). Processing is done through templates. There are predefined templates for determining the data required for user accounts included in the default installation. You can customize templates as required.

For detailed information about account definitions, see the One Identity Manager Target System Base Module Administration Guide.

The following steps are required to implement an account definition:

- Creating an account definition
- Creating manage levels
- Creating a mapping rule for IT operating data
- Entering the IT operating data
- Assigning account definitions to employees
- Assigning account definitions to a target system

If user accounts are managed in the SAP R/3 environment through the central user administration (CUA), you can use account definitions to grant user accounts access to the child systems and the central system. For more information, see Central user administration in One Identity Manager on page 112.

Creating an account definition

To create a new account definition

1. In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list. Select Change master data.
   -OR-
   Click in the result list.
3. Enter the account definition's master data.
4. Save the changes.

Detailed information about this topic

- Master data for an account definition on page 59

Master data for an account definition

Enter the following data for an account definition:
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account definition</td>
<td>Account definition name.</td>
</tr>
<tr>
<td>User account table</td>
<td>Table in the One Identity Manager schema that maps user accounts. For an account definition to create user accounts, select SAPUser. To guarantee access to the tenants of central user administration (CUA) system, select SAPUserMandant.</td>
</tr>
<tr>
<td>Target system</td>
<td>Target system to which the account definition applies.</td>
</tr>
<tr>
<td>Required account definition</td>
<td>Required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is automatically requested or assigned with it. If you want the account definition to provide access to tenants of the CUA system, assign the account definitions with which the user accounts are created in the central system. A user account is then created in the central system if the employee does not yet have a user account. For an account definition to create user accounts, leave this field empty.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Manage level (initial)</td>
<td>Manage level to use by default when you add new user accounts. If the account definition is valid for the child system of a CUA system, assign the Unmanaged manage level.</td>
</tr>
<tr>
<td>Risk index</td>
<td>Value for evaluating the risk of account definition assignments to employees. Enter a value between 0 and 1. This input field is only visible if the configuration parameter QER</td>
</tr>
<tr>
<td>Service item</td>
<td>Service item through which you can request the account definition in the IT Shop. Assign an existing service item or add a new one.</td>
</tr>
<tr>
<td>IT Shop</td>
<td>Specifies whether the account definition can be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. The account definition can also be assigned directly to employees and roles outside of IT Shop.</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>Specifies whether the account definition can only be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Automatic assignment to employees</td>
<td>Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added.</td>
</tr>
<tr>
<td>Retain account definition if permanently disabled</td>
<td>Specifies the account definition assignment to permanently disabled employees.</td>
</tr>
<tr>
<td>Retain account definition if temporarily disabled</td>
<td>Specifies the account definition assignment to temporarily disabled employees.</td>
</tr>
<tr>
<td>Retain account definition on deferred deletion</td>
<td>Specifies the account definition assignment on deferred deletion of employees.</td>
</tr>
<tr>
<td>Retain account definition on security risk</td>
<td>Specifies the account definition assignment to employees posing a security risk.</td>
</tr>
<tr>
<td>Resource type</td>
<td>Resource type for grouping account definitions.</td>
</tr>
</tbody>
</table>
### Creating manage levels

Specify the manage level for an account definition for managing user accounts. The user account’s manage level specifies the extent of the employee’s properties that are inherited by the user account. This allows an employee to have several user accounts in one target system, for example:

- Default user account that inherits all properties from the employee
- Administrative user account that is associated to an employee but should not inherit the properties from the employee.

One Identity Manager supplies a default configuration for manage levels:

- **Unmanaged**: User accounts with the Unmanaged manage level are linked to the employee but they do no inherit any further properties. When a new user account is added with this manage level and an employee is assigned, some of the employee’s properties are transferred initially. If the employee properties are changed at a later date, the changes are not passed onto the user account.

- **Full managed**: User accounts with the Full managed manage level inherit defined properties of the assigned assigned employee. When a new user account is created with this manage level and an employee is assigned, the employee’s properties are transferred in an initial state. If the employee properties are changed at a later date, the changes are passed onto the user account.

**NOTE:** The Full managed and Unmanaged are analyzed in templates. You can customize the supplied templates in the Designer.

You can define other manage levels depending on your requirements. You need to amend the templates to include manage level approaches.

Specify the effect of temporarily or permanently disabling, deleting or the security risk of an employee on its user accounts and group memberships for each manage level. For detailed information about manage levels, see the One Identity Manager Target System Base Module Administration Guide.

- Employee user accounts can be locked when they are disabled, deleted or rated as a security risk so that permissions are immediately withdrawn. If the employee is reactivated, the user accounts are also reactivated.

- You can also define group membership inheritance. Inheritance can be discontinued if desired when, for example, the employee’s user accounts are disabled and therefore cannot be members in groups. During this time, no inheritance processes should be calculated for this employee. Existing group memberships are deleted!
To assign manage levels to an account definition

1. In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list.
3. Select Assign manage level.
4. Assign the manage levels in Add assignments.
   - OR -
   Delete the manage levels in Remove assignments.
5. Save the changes.

**IMPORTANT:** The Unmanaged manage level is assigned automatically when you create an account definition and it cannot be removed.

To edit a manage level

1. Select SAP R/3 | Basic configuration data | Account definitions | Manage levels.
2. Select the manage level in the result list. Select Change master data.
   - OR -
   Click in the result list.
3. Edit the manage level's master data.
4. Save the changes.

Detailed information about this topic

- Master data for a manage level on page 63

Master data for a manage level

Enter the following data for a manage level.

Table 26: Master data for manage levels

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage level</td>
<td>Name of the manage level.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>IT operating data overwrites</td>
<td>Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are:</td>
</tr>
<tr>
<td></td>
<td>• Never: Data is not updated.</td>
</tr>
<tr>
<td></td>
<td>• Always: Data is always updated.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Retain groups if temporarily disabled</td>
<td>Specifies whether user accounts of temporarily disabled employees retain their group memberships.</td>
</tr>
<tr>
<td>Lock user accounts if temporarily disabled</td>
<td>Specifies whether user accounts of temporarily disabled employees are locked.</td>
</tr>
<tr>
<td>Retain groups if permanently disabled</td>
<td>Specifies whether user accounts of permanently disabled employees retain group memberships.</td>
</tr>
<tr>
<td>Lock user accounts if permanently disabled</td>
<td>Specifies whether user accounts of permanently disabled employees are locked.</td>
</tr>
<tr>
<td>Retain groups on deferred deletion</td>
<td>Specifies whether user accounts of employees marked for deletion retain their group memberships.</td>
</tr>
<tr>
<td>Lock user accounts if deletion is deferred</td>
<td>Specifies whether user accounts of employees marked for deletion are locked.</td>
</tr>
<tr>
<td>Retain groups on security risk</td>
<td>Specifies whether user accounts of employees posing a security risk retain their group memberships.</td>
</tr>
<tr>
<td>Lock user accounts if security is at risk</td>
<td>Specifies whether user accounts of employees posing a security risk are locked.</td>
</tr>
<tr>
<td>Retain groups if user account disabled</td>
<td>Specifies whether locked user accounts retain their group memberships.</td>
</tr>
</tbody>
</table>

**Creating a mapping rule for IT operating data**

An account definition specifies which rules are used to form the IT operating data and which default values will be used if no IT operating data can be found through the employee's primary roles.

The following IT operating data is used in the One Identity Manager default configuration for automatic creating and modifying of user accounts for an employee in the target system.

- Groups can be inherited
- Identity
- Privileged user account
To create a mapping rule for IT operating data

1. In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list.
3. Select Edit IT operating data mapping and enter the following data.

Table 27: Mapping rule for IT operating data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column</td>
<td>User account property for which the value is set. In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For detailed information, see the One Identity Manager Target System Base Module Administration Guide.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies which roles to use in order to find the user account properties. You have the following options:</td>
</tr>
<tr>
<td></td>
<td>• Primary department</td>
</tr>
<tr>
<td></td>
<td>• Primary location</td>
</tr>
<tr>
<td></td>
<td>• Primary cost center</td>
</tr>
<tr>
<td></td>
<td>• Primary business roles</td>
</tr>
<tr>
<td></td>
<td>![NOTE]: Only use the primary business role if the Business Roles Module is installed.</td>
</tr>
<tr>
<td></td>
<td>• Empty</td>
</tr>
<tr>
<td></td>
<td>If you select a role, you must specify a default value and set the option Always use default value.</td>
</tr>
<tr>
<td>Default value</td>
<td>Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.</td>
</tr>
<tr>
<td>Always use</td>
<td>Specifies whether user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.</td>
</tr>
<tr>
<td>default value</td>
<td></td>
</tr>
<tr>
<td>Notify when</td>
<td>Specifies whether email notification to a defined mailbox is sent when the default value is used. The Employee - new user account with default properties created mail template is used. To change the mail template, adjust the TargetSystem</td>
</tr>
<tr>
<td>applying the</td>
<td></td>
</tr>
<tr>
<td>standard</td>
<td></td>
</tr>
</tbody>
</table>

4. Save the changes.
Entering the IT operating data

To create user accounts with the **Full managed** manage level, the required IT operating data must be determined. The operating data required to automatically supply an employee with IT resources is shown in the business roles, departments, locations or cost centers. An employee is assigned a primary business role, primary location, primary department or primary cost center. The necessary IT operating data is ascertained from these assignments and used in creating the user accounts. Default values are used if valid IT operating data cannot be found over the primary roles.

You can also specify IT operating data directly for a specific account definition.

**Example**

Normally, each employee in department A obtains a default user account in the client A. In addition, certain employees in department A obtain administrative user accounts in the client A.

Create an account definition A for the default user account of the client A and an account definition B for the administrative user account of client A. Specify the property "Department" in the IT operating data formatting rule for the account definitions A and B in order to determine the valid IT operating data.

Specify the effective IT operating data of department A for the client A. This IT operating data is used for standard user accounts. In addition, specify the effective account definition B IT operating data for department A. This IT operating data is used for administrative user accounts.

**To define IT operating data**

1. In Manager, select the role in the **Organizations** or **Business roles** category.
2. Select the **Edit IT operating data** task.
3. Click **Add** and enter the following data.

**Table 28: IT operating data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effects on</td>
<td>IT operating data application scope. The IT operating data can be used for a target system or a defined account definition. To specify an application scope</td>
</tr>
<tr>
<td></td>
<td>a. Click ➔ next to the text box.</td>
</tr>
<tr>
<td></td>
<td>b. Under <strong>Table</strong>, select the table that maps the target system for select the TSBAccountDef table for an account definition.</td>
</tr>
<tr>
<td></td>
<td>c. Select the specific target system or account definition under <strong>Effects on</strong>.</td>
</tr>
<tr>
<td></td>
<td>d. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Column</td>
<td>User account property for which the value is set. In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For detailed information, see the One Identity Manager Target System Base Module Administration Guide.</td>
</tr>
<tr>
<td>Value</td>
<td>Concrete value which is assigned to the user account property.</td>
</tr>
</tbody>
</table>

4. Save the changes.

**Modify IT operating data**

If IT operating data changes, you must transfer these changes to the existing user accounts. To do this, templates must be rerun on the affected columns. Before you can run the templates, you can check what effect a change to the IT operating data has on the existing user accounts. You can decide whether the change is transferred to the One Identity Manager database in the case of each affected column in each affected database.

**Prerequisites**

- The IT operating data of a department, cost center, business role, or a location was changed.
- OR -
- The default values in the IT operating data template were modified for an account definition.

**NOTE:** If the assignment of an employee to a primary department, cost center, business role or to a primary location changes, the templates are automatically executed.
To execute the template

1. In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list.
3. Select Execute templates in the task view
   This displays a list of all user account, which are created through the selected account definition and whose properties are changed by modifying the IT operating data.

   Old value: Current value of the object property.
   New value: Value that the object property would have following modification of the IT operating data.
   Selection: Specifies whether the modification shall be adopted for the user account.

4. Mark all the object properties in the selection column that will be given the new value.
5. Click Apply.
   The templates are applied to all selected user accounts and properties.

Assigning account definitions to employees

Account definitions are assigned to company employees. Indirect assignment is the default method for assigning account definitions to employees. Account definitions are assigned to departments, cost centers, locations or roles. The employees are categorized into these departments, cost centers, locations or roles depending on their function in the company and thus obtain their account definitions. To react quickly to special requests, you can assign individual account definitions directly to employees.

You can automatically assign special account definitions to all company employees. It is possible to assign account definitions to the IT Shop as requestable products. A department manager can then request user accounts from the Web Portal for his staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or directly or added as products in the IT Shop.

In the One Identity Manager default installation, the processes are checked at the start to see if the employee already has a user account in the target system that has an account definition. If no user account exists, a new user account is created with the account definition’s default manage level.

NOTE: If a user account already exists and is disabled, then it is re-enabled. You have to alter the user account manage level afterwards in this case.
Prerequisites for indirect assignment of account definitions to employees

- Assignment of employees and account definitions is permitted for role classes (department, cost center, location or business role).

**NOTE:** As long as an account definition for an employee is valid, the employee retains the user account that was created by it. If the assignment of an account definition is removed, the user account that was created from this account definition is deleted.

For detailed information about preparing role classes to be assigned, see the One Identity Manager Identity Management Base Module Administration Guide.

Detailed information about this topic

- Assigning account definitions to departments, cost centers, and locations on page 69
- Assigning an account definition to business roles on page 70
- Assigning account definitions to all employees on page 70
- Assigning account definitions directly to employees on page 71
- Assigning account definitions to a target system on page 73

Assigning account definitions to departments, cost centers, and locations

**To add account definitions to hierarchical roles**

1. In Manager, select **SAP R/3 | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost centers** tab.

**TIP:** In the **Remove assignments** area, you can remove the assignment of organizations.

**To remove an assignment**

- Select the organization and double click ☑.

5. Save the changes.
Assigning an account definition to business roles

Installed modules: Business Roles Module

To add account definitions to hierarchical roles

1. In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list.
3. Select Assign business roles in the task view.
4. Assign business roles in Add assignments.
   - TIP: In the Remove assignments area, you can remove the assignment of business roles.
   - To remove an assignment
     - Select the business role and double click.
5. Save the changes.

Assigning account definitions to all employees

To assign an account definition to all employees

1. In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list.
3. Select Change master data.
4. Set Automatic assignment to employees on General.
   - IMPORTANT: Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system.
5. Save the changes.

The account definition is assigned to every employee that is not marked as external. New employees automatically obtain this account definition as soon as they are added. The assignment is calculated by the DBQueue Processor.

- NOTE: Disable Automatic assignment to employees to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing assignments remain intact.
Assigning account definitions directly to employees

To assign an account definition directly to employees

1. In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list.
3. Select Assign to employees in the task view.
4. Assign employees in Add assignments.
   - TIP: In the Remove assignments area, you can remove the assignment of employees.
   - To remove an assignment
     - Select the employee and double-click ✗.
5. Save the changes.

Assigning account definitions to system roles

Installed modules: System Roles Module

- NOTE: Account definitions with Only use in IT Shop can only be assigned to system roles that also have this option set.

To add account definitions to a system role

1. In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list.
3. Select Assign system roles in the task view.
4. Assign system roles in Add assignments.
   - TIP: In the Remove assignments area, you can remove the assignment of system roles.
   - To remove an assignment
     - Select the system role and double click ✗.
5. Save the changes.
Adding account definitions in the IT Shop

A account definition can be requested by shop customers when it is assigned to an IT Shop shelf. To ensure it can be requested, further prerequisites need to be guaranteed.

- The account definition must be labeled with the **IT Shop** option.
- The account definition must be assigned to a service item.

**TIP:** In Web Portal, all products that can be requested are grouped together by service category. To make the account definition easier to find in Web Portal, assign a service category to the service item.

- If the account definition is only assigned to employees using IT Shop assignments, you must also set **Only for use in IT Shop**. Direct assignment to hierarchical roles may not be possible.

**NOTE:** IT Shop administrators can assign account definitions to IT Shop shelves if login is role-based. Target system administrators are not authorized to add account definitions in the IT Shop.

To add an account definition to the IT Shop

1. In Manager, select **SAP R/3 | Basic configuration data | Account definitions | Account definitions** (non-role-based login).
   - OR -
   In Manager, select **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop**.
4. Assign the account definitions to the IT Shop shelves in **Add assignments**.
5. Save the changes.

To remove an account definition from individual IT Shop shelves

1. In Manager, select **SAP R/3 | Basic configuration data | Account definitions | Account definitions** (non-role-based login).
   - OR -
   In Manager, select **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop**.
4. Remove the account definitions from the IT Shop shelves in **Remove assignments**.
5. Save the changes.
To remove an account definition from all IT Shop shelves

1. In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions (non-role-based login).
   - OR -
   In Manager, select Entitlements | Account definitions (role-based login).
2. Select an account definition in the result list.
3. Select Remove from all shelves (IT Shop).
4. Confirm the security prompt with Yes.
5. Click OK.

The account definition is removed from all shelves by One Identity Manager Service. All requests and assignment requests with this account definition are canceled in the process.

For more detailed information about request from company resources through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Related topics

- Master data for an account definition on page 59
- Assigning account definitions to departments, cost centers, and locations on page 69
- Assigning an account definition to business roles on page 70
- Assigning account definitions directly to employees on page 71
- Assigning account definitions to system roles on page 71

Assigning account definitions to a target system

**NOTE:** To use automatic employee assignment for central user administration (CUA) user accounts, assign and account definition to the CUA central system using the SAPUser user table.

The following prerequisites must be fulfilled if you implement automatic assignment of user accounts and employees resulting in administered user accounts (state Linked configured):

- The account definition is assigned to the target system.
- The account definition has the default manage level.

User accounts are only linked to the employee (Linked) if no account definition is given. This is the case on initial synchronization, for example.
To assign the account definition to a target system

1. In Manager, select the tenant in SAP R/3 | Tenants.
2. Select Change master data.
3. Select the account definition for user accounts from Account definition (initial).
4. Save the changes.

Deleting an account definition

You can delete account definitions if they are not assigned to target systems, employees, hierarchical roles or any other account definitions.

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
   a. In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions.
   b. Select an account definition in the result list.
   c. Select Change master data.
   d. Disable Automatic assignment to employees on the General tab.
   e. Save the changes.
2. Remove direct assignments of the account definition to employees.
   a. In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions.
   b. Select an account definition in the result list.
   c. Select Assign to employees in the task view.
   d. Remove employees from Remove assignments.
   e. Save the changes.
3. Remove the account definition’s assignments to departments, cost centers and locations.
   a. In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions.
   b. Select an account definition in the result list.
   c. Select Assign organizations.
   d. In Remove assignments, remove the relevant departments, cost centers, and locations.
   e. Save the changes.
4. Remove the account definition’s assignments to business roles.
   - In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions.
   - Select an account definition in the result list.
   - Select Assign business roles.
     Remove the business roles in Remove assignments.
   - Save the changes.

5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.
   
   For more detailed information about unsubscribing requests, see the One Identity Manager Web Portal User Guide.
   
   **To remove an account definition from all IT Shop shelves**
   - In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions (non-role-based login).
     - OR -
       In Manager, select Entitlements | Account definitions (role-based login).
   - Select an account definition in the result list.
   - Select Remove from all shelves (IT Shop).
   - Confirm the security prompt with Yes.
   - Click OK.
     
     The account definition is removed from all shelves by One Identity Manager Service. All requests and assignment requests with this account definition are canceled in the process.

6. Remove the account definition assignment as required account definition for another account definition. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.
   - In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions.
   - Select an account definition in the result list.
   - Select Change master data.
   - Remove the account definition in the Required account definition menu.
   - Save the changes.

7. Remove the account definition's assignments to target systems.
   - In Manager, select the tenant in SAP R/3 | Tenants.
   - Select Change master data.
   - Remove the assigned account definitions on the General tab.
   - Save the changes.
8. Delete the account definition.
   a. In Manager, select SAP R/3 | Basic configuration data | Account definitions | Account definitions.
   b. Select an account definition in the result list.
   c. Click to delete an account definition.

Basic data for user account administration

The One Identity Manager supplies the following basic data for user administration, by default:
- User account types on page 76
- External identifier types on page 77

Other basic data is read from SAP R/3 during synchronization, if configured, and cannot be editing in One Identity Manager. This merely allows assignment to an SAP user account. These include:
- Parameters on page 78
- Printers on page 78
- Cost centers on page 78
- Start menus on page 79
- Companies on page 79
- Login languages on page 79
- Licenses on page 80
- Special versions on page 81

Certain user account properties can be defined as default for all user accounts through the configuration settings. These include:
- Initial password for new SAP user accounts on page 91
- Email notifications about login data on page 93

User account types

The user account types are available in One Identity Manager by default. SAP R/3 recognizes the user account types listed below.
Table 29: User Account Types

<table>
<thead>
<tr>
<th>User account type</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialog (A)</td>
<td>Dialog user in a system.</td>
</tr>
<tr>
<td>System (B)</td>
<td>Background processing within a system.</td>
</tr>
<tr>
<td>Communication (C)</td>
<td>Communication between systems without a dialog.</td>
</tr>
<tr>
<td>Service (S)</td>
<td>Common user account for anonymous system access, for example. User account of this type should have heavily restricted access permissions.</td>
</tr>
<tr>
<td>Reference (L)</td>
<td>Common user account for additional granting of permissions.</td>
</tr>
</tbody>
</table>

The default user account type for new user accounts is specified in "TargetSystem\SAPR3\UserDefaults\Ustyp".

**To modify the default user account type**

- Edit the value of "TargetSystem\SAPR3\UserDefaults\Ustyp" in Designer.

External identifier types

External authentication methods for logging on to a system can be used in SAP R/3. One Identity Manager supplies the following types as user identifiers to find the login data necessary for different authentication mechanisms for external systems on an SAP system:

Table 30: External identifier types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DN</td>
<td>Distinguished Name for X.509.</td>
</tr>
<tr>
<td>NT</td>
<td>Windows NTLM or password verification with the Windows domain controller.</td>
</tr>
<tr>
<td>LD</td>
<td>LDAP bind &lt;user defined&gt; (For other external authentication mechanisms).</td>
</tr>
<tr>
<td>SA</td>
<td>SAML Token.</td>
</tr>
</tbody>
</table>

**To specify a default type for external identifiers**

- Set "TargetSystem\SAPR3\UserDefaults\ExtID_Type" in Designer and specify a value.
Parameters

Parameters can be loaded into the One Identity Manager database and assigned to user account by synchronization.

To display parameters

1. Select SAP R/3 | Parameters.
2. Select the parameter in the result list. Select Change master data.

Table 31: Parameter properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>System to which the parameter belongs.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Parameter name.</td>
</tr>
<tr>
<td>Text</td>
<td>Description of the parameter.</td>
</tr>
</tbody>
</table>

Related topics

- Assigning parameters on page 124

Printers

To display a printer

1. Select SAP R/3 | Printers.
2. Select the printer in the result list.

The printer's properties, assigned SAP system and assigned user accounts are displayed on the overview form.

Cost centers

To display a cost center

1. Select SAP R/3 | Cost centers.
2. Select the cost center in the result list.

The cost center properties and assigned client are displayed on the overview form.
Start menus

To display a start menu

1. Select SAP R/3 | Start menus.
2. Select the start menu in the result list.

The start menu's properties, assigned client and assigned user accounts are displayed on the overview form.

Companies

To display a company

1. Select SAP R/3 | Companies.
2. Select the company in the result list.

The company's properties, assigned client and assigned user accounts are displayed on the overview form.

Login languages

To display a login language

1. Select SAP R/3 | Basic configuration data | Login languages.
2. Select the login language in the result list.

The login language's properties, the associated SAP system and assigned user accounts are displayed on the overview form.

Security policies

You can load security policies into the One Identity Manager database using synchronization and assign then to a user account.

To display security policies

1. Select SAP R/3 | Security policies.
2. Select the security policy in the result list. Select Change master data.

Valid security policy attributes, the assigned client, and user account accounts are displayed on the overview form.
Communication types

Communication types can be loaded into the One Identity Manager database by synchronization and assigned to user accounts.

To display communication types

1. Select SAP R/3 | Communication types.
2. Select the communication type from the result list.

The assign user accounts are shown on the overview form.

Licenses

Licenses are required for user account system measurement. Select the following objects in the synchronization configuration to be able to synchronize licenses and their properties with the database after initial migration.

To enter a rating for a license

1. Select SAP R/3 | Licenses.
2. Select the license in the result list. Select Change master data.
3. Enter a value in Rating.
4. Save the changes.

The following information is shown for Licenses:

Table 32: License master data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>Unique license identifier. Used to determine the system measurement rating if no license rating is entered.</td>
</tr>
<tr>
<td>System</td>
<td>Associated SAP system.</td>
</tr>
<tr>
<td>User type</td>
<td>User type of the SAP system to which the license applies.</td>
</tr>
<tr>
<td>Price list (token)</td>
<td>Number in the price list.</td>
</tr>
<tr>
<td>Price list (text)</td>
<td>Description in the price list.</td>
</tr>
<tr>
<td>Rating</td>
<td>License rating as alphanumeric string. Enter any alphanumeric character string. Case sensitivity is not taken into account when determining the rating for system measurement. The license rating is evaluated when the system measurement ratings are</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>determined. If no rating is entered the license ID for determining the rating for system measurement is used.</td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>Specifies whether the license is enabled.</td>
</tr>
<tr>
<td>Special version</td>
<td>Specifies whether special versions can be selected for this license.</td>
</tr>
<tr>
<td>Country surcharge</td>
<td>Specifies whether country surcharges can be selected for this license.</td>
</tr>
</tbody>
</table>

**Detailed information about this topic**
- Providing system measurement data on page 182

**Special versions**

If special versions are installed in an SAP R/3 environment for license extension, user accounts for system measurement must be classified accordingly.

You can see the CUA assignment to user accounts on the special version overview form. Navigate to the user account with the mouse and edit the special version assignment.

**To obtain an overview of an e special version**
1. Select SAP R/3 | Special versions.
2. Select the special version in the result list.

**Password policies for SAP user accounts**

One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

Predefined password policies are supplied with the default installation that you can user or customize if required. You can also define your own password policies.

**Detailed information about this topic**
- Predefined password policies on page 82
- Using a password policy on page 83
- Editing password policies on page 85
- Custom scripts for password requirements on page 88
Predefined password policies

You can customize predefined password policies to meet your own requirements, if necessary.

Password for logging in to One Identity Manager

The One Identity Manager password policy is applied for logging in to One Identity Manager. This password policy defined the settings for the system user passwords (DialogUser.Password and Person.DialogUserPassword) as well as the access code for a one off log in on the Web Portal (Person.Passcode).

**NOTE:** The One Identity Manager password policy is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts or system users.

For detailed information about password policies for employees, see the One Identity Manager Identity Management Base Module Administration Guide.

Password policy for forming employees' central passwords

An employee's central password is formed from the target system specific user accounts by respective configuration. The Employee central password policy password policy defines the settings for the (Person.CentralPassword) central password. Members of the Identity Management | Employees | Administrators application role can adjust this password policy.

**IMPORTANT:** Ensure that the Employee central password policy password policy does not violate the system-specific requirements for passwords.

For detailed information about password policies for employees, see the One Identity Manager Identity Management Base Module Administration Guide.

Password policies for user accounts

Predefined password policies are provided, which you can apply to the user account password columns of the user accounts.

**IMPORTANT:** If you do not use password policies that are specific to the target system, the One Identity Manager password policy standard policy applies. In this case, ensure that the default policy does not violate the target systems requirements.
NOTE: When you update One Identity Manager version 7.x to One Identity Manager version 8.1.1, the configuration parameter settings for forming passwords are passed on to the target system specific password policies.

The SAP R/3 password policy is predefined for SAP R/3. You can apply this password policy to SAP user accounts (SAPUser.Password) of an SAP client.

If the clients' password requirements differ, it is recommended that you set up your own password policies for each client.

Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

Using a password policy

The SAP R/3 password policy is predefined for SAP R/3. You can apply this password policy to SAP user accounts (SAPUser.Password) of an SAP client.

If the clients' password requirements differ, it is recommended that you set up your own password policies for each client.

Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

The password policy that is to be used for a user account is determined in the following sequence:

1. Password policy of the account definition of the user account
2. Password policy of the manage level of the user account
3. Password policy for the client of the user account
4. Password policy One Identity Manager password policy (default policy)

IMPORTANT: If you do not use password policies that are specific to the target system, the One Identity Manager password policy standard policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

To reassign a password policy

1. In the Manager, select the SAP R/3 | Basic configuration data | Password policies category.
2. Select the password policy in the result list.
3. Select Assign objects.
4. Click **Add** in the **Assignments** section and enter the following data.

**Table 33: Assigning a Password Policy**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply to</td>
<td>Application scope of the password policy.</td>
</tr>
<tr>
<td></td>
<td><strong>To specify an application scope</strong></td>
</tr>
<tr>
<td></td>
<td>a. Click ➔ next to the text box.</td>
</tr>
<tr>
<td></td>
<td>b. Select one of the following references under Table:</td>
</tr>
<tr>
<td></td>
<td>• The table that contains the base objects of synchronization.</td>
</tr>
<tr>
<td></td>
<td>• To apply the password policy based on the account definition,</td>
</tr>
<tr>
<td></td>
<td>select the TSBAccountDef table.</td>
</tr>
<tr>
<td></td>
<td>• Select the TSBBehavior table to apply the password policy</td>
</tr>
<tr>
<td></td>
<td>based on the manage level.</td>
</tr>
<tr>
<td></td>
<td>c. Select the table that contains the base objects under <strong>Apply to</strong>.</td>
</tr>
<tr>
<td></td>
<td>• If you have selected the table containing the base objects of</td>
</tr>
<tr>
<td></td>
<td>synchronization, next select the specific target system.</td>
</tr>
<tr>
<td></td>
<td>• If you have selected the TSBAccountDef table, next select the</td>
</tr>
<tr>
<td></td>
<td>specific account definition.</td>
</tr>
<tr>
<td></td>
<td>• If you have selected the TSBBehavior table, next select the</td>
</tr>
<tr>
<td></td>
<td>specific manage level.</td>
</tr>
<tr>
<td></td>
<td>d. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Password</td>
<td>The password column's identifier.</td>
</tr>
<tr>
<td>Password</td>
<td>policy</td>
</tr>
<tr>
<td>Password</td>
<td>The identifier of the password policy to be used.</td>
</tr>
<tr>
<td>policy</td>
<td></td>
</tr>
</tbody>
</table>

5. Save the changes.

**To change a password policy's assignment**

1. In the Manager, select the **SAP R/3 | Basic configuration data | Password policies** category.
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Select the assignment you want to change in **Assignments**.
5. Select the new password policy to apply from the **Password Policies** menu.
6. Save the changes.
Editing password policies

To edit a password policy

1. In the Manager, select the SAP R/3 | Basic configuration data | Password policies category.
2. Select the password policy in the result list and select Change master data.
   - OR -
   Click in the result list.
3. Edit the password policy's master data.
4. Save the changes.

Detailed information about this topic

- General master data for a password policy on page 85
- Policy settings on page 86
- Character classes for passwords on page 87
- Custom scripts for password requirements on page 88

General master data for a password policy

Enter the following master data for a password policy.

Table 34: Master data for a password policy

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Password policy name. Translate the given text using the button.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation. Translate the given text using the button.</td>
</tr>
<tr>
<td>Error Message</td>
<td>Custom error message outputted if the policy is not fulfilled. Translate the given text using the button.</td>
</tr>
<tr>
<td>Owner (Application Role)</td>
<td>Application roles whose members can configure the password policies.</td>
</tr>
<tr>
<td>Default policy</td>
<td>Mark as default policy for passwords.</td>
</tr>
</tbody>
</table>

NOTE: The One Identity Manager password policy is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts or system users.
Policy settings

Define the following settings for a password policy on the **Password** tab.

**Table 35: Policy settings**

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial password</td>
<td>Initial password for newly created user accounts. If a password is not entered or if a random password is not generated when a user account is created, the initial password is used.</td>
</tr>
<tr>
<td>Password confirmation</td>
<td>Reconfirm password.</td>
</tr>
<tr>
<td>Minimum Length</td>
<td>Minimum length of the password. Specify the number of characters a password must have.</td>
</tr>
<tr>
<td>Max. length</td>
<td>Maximum length of the password. Specify the number of characters a password can have.</td>
</tr>
<tr>
<td>Max. errors</td>
<td>Maximum number of errors. Set the number of invalid passwords. Only taken into account when logging in to One Identity Manager. This data is only taken into account if the One Identity Manager login was through a system user or employee based authentication module. If a user has reached the number of maximum failed logins, the employee or system user can no longer log in to One Identity Manager. You can reset the passwords of employees and system users who have been blocked in Password Reset Portal. For more detailed information, see the <em>One Identity Manager Web Portal User Guide</em>.</td>
</tr>
<tr>
<td>Validity period</td>
<td>Maximum age of the password. Enter the length of time a password can be used before it expires.</td>
</tr>
<tr>
<td>Password history</td>
<td>Enter the number of passwords to be saved. If, for example, a value of 5 is entered, the user's last five passwords are stored.</td>
</tr>
<tr>
<td>Minimum password strength</td>
<td>Specifies how secure the password must be. The higher the password strength, the more secure it is. The value 0 means that the password strength is not tested. The values 1, 2, 3 and 4 specify the required complexity of the password. The value 1 represents the lowest requirements in terms of password strength. The value 4 requires the highest level of complexity.</td>
</tr>
<tr>
<td>Name properties denied</td>
<td>Specifies whether name properties are permitted or not permitted in the password. If this option is enabled, name</td>
</tr>
</tbody>
</table>
properties are not permitted in passwords. The values of the columns for which the Contains name properties for password check option is set are taken into account. Adjust this option in the column definition in Designer. For more detailed information, see the One Identity Manager Configuration Guide.

Character classes for passwords

Use the Character classes tab to specify which characters are permitted for a password.

Table 36: Character classes for passwords

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min. number letters</td>
<td>Specifies the minimum number of alphabetical characters the password must contain.</td>
</tr>
<tr>
<td>Min. number lowercase</td>
<td>Specifies the minimum number of lowercase letters the password must contain.</td>
</tr>
<tr>
<td>Min. number uppercase</td>
<td>Specifies the minimum number of uppercase letters the password must contain.</td>
</tr>
<tr>
<td>Min. number digits</td>
<td>Specifies the minimum number of digits the password must contain.</td>
</tr>
<tr>
<td>Min. number special characters</td>
<td>Specifies the minimum number of special characters the password must contain.</td>
</tr>
<tr>
<td>Permitted special characters</td>
<td>List of permitted characters.</td>
</tr>
<tr>
<td>Max. identical characters in total</td>
<td>Maximum number of identical characters that can be present in the password in total.</td>
</tr>
<tr>
<td>Max. identical characters in succession</td>
<td>Maximum number of identical character that can be repeated after each other.</td>
</tr>
<tr>
<td>Denied special characters</td>
<td>List of characters, which are not permitted.</td>
</tr>
<tr>
<td>Lowercase not allowed</td>
<td>Specifies whether the password can contain lower case letters. This setting is only applies when passwords are generated.</td>
</tr>
<tr>
<td>Uppercase not allowed</td>
<td>Specifies whether the password can contain upper case letters. This setting is only applies when passwords are generated.</td>
</tr>
<tr>
<td>Digits not allowed</td>
<td>Specifies whether the password can contain digits. This setting is only applies when passwords are generated.</td>
</tr>
<tr>
<td>Property</td>
<td>Meaning</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Special characters not allowed</td>
<td>Specifies whether the password can contain special characters. This setting is only applies when passwords are generated.</td>
</tr>
</tbody>
</table>

### Custom scripts for password requirements

You can implement custom scripts for testing and generating password if the password requirements cannot be mapped with the existing settings options. Scripts are applied in addition to the other settings.

#### Detailed information about this topic

- Script for checking a password on page 88
- Script for generating a password on page 89

### Script for checking a password

You can implement a check script if additional policies need to be used for checking a password, which cannot be mapped with the available settings.

#### Syntax for Check Scripts

```vbnet
Public Sub CCC_CustomPwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
With parameters:  
  policy = password policy object  
  spwd = password to test
  TIP: To use a base object, take the property Entity of the PasswordPolicy class.

End Sub
```

#### Example for a script for testing a password

A password cannot start with ? or !. The script checks a given password for validity.

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

To use a custom script for checking a password
1. Create your script in the category Script Library in the Designer.
2. Edit the password policy.
   a. In the Manager, select the SAP R/3 | Basic configuration data | Password policies category.
   b. Select the password policy in the result list.
   c. Select Change master data.
   d. Enter the name of the script to be used to check a password in the Check script input field on the Scripts tab.
   e. Save the changes.

Related topics
- Script for generating a password on page 89

Script for generating a password
You can implement a generating script if additional policies need to be used for generating a random password, which cannot be mapped with the available settings.

Syntax for generating script
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
With parameters:
policy = password policy object
spwd = generated password

TIP: To use a base object, take the property Entity of the PasswordPolicy class.

Example for a script to generate a password
In random passwords, the script replaces the ? and ! characters, which are not permitted.
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
Dim pwd = spwd.ToInsecureArray()
' replace invalid characters at first position
If pwd.Length>0
    If pwd(0)="?" Or pwd(0)="!"
        spwd.SetAt(0, CChar("_"))
    End If
End If
End Sub

**To use a custom script for generating a password**

1. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
   a. In the Manager, select the **SAP R/3 | Basic configuration data | Password policies** category.
   b. Select the password policy in the result list.
   c. Select **Change master data**.
   d. Enter the name of the script to be used to generate a password in the **Generating script** input field on the **Scripts** tab.
   e. Save the changes.

**Related topics**

- Script for checking a password on page 88

**Excluded list for passwords**

You can add words to a list of restricted terms to prohibit them from being used in passwords.

**NOTE:** The restricted list applies globally to all password policies.

**To add a term to the restricted list**

1. Select **Base Data | Security settings | Restricted passwords** in Designer.
2. Create a new entry with **Object | New** and enter the term to excluded to the list.
3. Save the changes.
Checking a password

When you test a password, all the password policy settings, custom scripts and the restricted passwords are taken into account.

To test whether a password conforms to the password policy

1. In the Manager, select the SAP R/3 | Basic configuration data | Password policies category.
2. Select the password policy in the result list.
3. Select Change master data.
4. Select the Test tab.
5. Select the table and object to be tested in Base object for test.
6. Enter a password in Enter password to test.
   A display next to the password shows whether it is valid or not.

Testing generation of a password

When you generate a password, all the password policy settings, custom scripts and the restricted passwords are taken into account.

To generate a password that conforms to the password policy

1. In the Manager, select the SAP R/3 | Basic configuration data | Password policies category.
2. Select the password policy in the result list.
3. Select Change master data.
4. Select the Test tab.
5. Click Generate.
   This generates and displays a password.

Initial password for new SAP user accounts

Table 37: Configuration parameters for formatting initial passwords for user accounts

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER\Person\UseCentralPassword</td>
<td>This configuration parameter specifies whether the employee’s central password is used in the user</td>
</tr>
<tr>
<td>Configuration parameter</td>
<td>Meaning</td>
</tr>
<tr>
<td>-------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>accounts. The employee’s central password is automatically</td>
<td>mapped to the employee’s user account in all permitted target systems. This excludes privileged user accounts, which are not updated.</td>
</tr>
<tr>
<td>QER\Person\UseCentralPassword\PermanentStore</td>
<td>This configuration parameter controls the storage period for central passwords. If the configuration parameter is enabled, the central password is stored in the One Identity Manager database and is used for new users. If the configuration parameter is disabled, the central password is deleted from the One Identity Manager database following publishing to the existing user accounts. The central password is not available for new user accounts.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\InitialRandomPassword</td>
<td>This configuration parameter specifies whether a random generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy.</td>
</tr>
</tbody>
</table>

You have the following possible options for issuing an initial password for a new SAP user account.

- Create user accounts manually and enter a password in their master data.
- Assign a randomly generated initial password to enter when you create user accounts.
  - Enable the **TargetSystem | SAPR3 | Accounts | InitialRandomPassword** configuration parameter in Designer.
  - Apply target system specific password policies and define the character sets that the password must contain.
  - Specify which employee will receive the initial password by email.
- Use the employee’s central password. The employee’s central password is mapped to the user account password. For detailed information about an employee’s central password, see *One Identity Manager Identity Management Base Module Administration Guide*. 
Email notifications about login data

Table 38: Configuration parameters for notifications about actions in the target system

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetSystem\SAPR3\Accounts\InitialRandomPassword\SendTo</td>
<td>This configuration parameter specifies to which employee the email with the random generated password should be sent (manager cost center/department/location/business role, employee’s manager or XUserInserted). If no recipient can be found, the password is sent to the address stored in the “TargetSystem\SAPR3\DefaultAddress” configuration parameter.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName</td>
<td>This configuration parameter contains the name of the mail template sent to provide users with the login data for their user accounts. The <strong>Employee - new user account created</strong> mail template is used.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword</td>
<td>This configuration parameter contains the name of the mail template sent to provide users with information about their initial password. The <strong>Employee - initial password for new user account</strong> mail template is used.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\DefaultAddress</td>
<td>The configuration parameter contains the recipient’s default email address for sending notifications about actions in the target system.</td>
</tr>
</tbody>
</table>

You can configure the login information for new user accounts to be sent by email to a specified person. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages. The mail texts in a mail template are defined in several languages, which means the recipient’s language can be taken into account when the email is generated. Mail templates are supplied in the default installation with which you can configure the notification procedure.
To use email notifications about login data

1. Ensure that the email notification system is configured in One Identity Manager. For more detailed information, see the One Identity Manager Installation Guide.

2. In Designer, enable the Common | MailNotification | DefaultSender configuration parameter and enter the sender address for sending the email notifications.

3. Ensure that all employees have a default email address. Notifications are sent to this address. For more detailed information, see the One Identity Manager Identity Management Base Module Administration Guide.

4. Ensure that a language can be determined for all employees. Only then can they receive email notifications in their own language. For more detailed information, see the One Identity Manager Identity Management Base Module Administration Guide.

When a randomly generated password is issued for the new user account, the initial login data for a user account is sent by email to a previously specified person.

To send initial login data by email

1. Set "TargetSystem\SAPR3\Accounts\InitialRandomPassword" in Designer.

2. Set "TargetSystem\SAPR3\Accounts\InitialRandomPassword\SendTo" in Designer and enter the message recipient as value.

3. Set "TargetSystem\SAPR3\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName" in Designer.

   By default, the message sent uses the mail template "Employee - new account created". The message contains the name of the user account.

4. Set "TargetSystem\SAPR3\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword" in Designer.

   By default, the message sent uses the mail template "Employee - initial password for new user account". The message contains the initial password for the user account.

   TIP: Change the value of the configuration parameter in order to use custom mail templates for these mails.

Editing a server

In order to handle SAP R/3 specific processes in One Identity Manager, the synchronization server and its server functions must be declared. You have several options for defining a server's functionality:

- Create an entry for the Job server in Designer under Base Data | Installation | Job server. For detailed information, see One Identity Manager Configuration.
Guide.

- Select an entry for the Job server in SAP R/3 | Basic configuration data | Server in Manager and edit the Job server master data.

Use this task if the Job server has already been declared in One Identity Manager and you want to configure special functions for the Job server.

**NOTE:** One Identity Manager must be installed, configured, and started in order for a server to execute its function in the One Identity Manager Service network. Proceed as described in the One Identity Manager Installation Guide.

**To edit a Job server and its functions**

1. In Manager, select the category SAP R/3 | Basic configuration data | Server.
2. Select the Job server entry in the result list.
3. Select Change master data.
4. Edit the Job server's master data.
5. Select Assign server functions in the task view and specify server functionality.
6. Save the changes.

**Detailed information about this topic**

- Master data for a Job server on page 95
- Specifying server functions on page 98

**Related topics**

- Setting up the synchronization server on page 18

**Master data for a Job server**

**NOTE:** All editing options are also available in Designer under Base Data | Installation | Job server.

**NOTE:** More properties may be available depending on which modules are installed.

**Table 39: Job Server Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Job server name.</td>
</tr>
<tr>
<td>Full server name</td>
<td>Full server name in accordance with DNS syntax. Example:</td>
</tr>
<tr>
<td>Property</td>
<td>Meaning</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Property</td>
<td><strong>&lt;Name of servers&gt;.&lt;Fully qualified domain name&gt;</strong></td>
</tr>
<tr>
<td>Target system</td>
<td>Computer account target system.</td>
</tr>
<tr>
<td>Language</td>
<td>Language of the server.</td>
</tr>
<tr>
<td>Server is cluster</td>
<td>Specifies whether the server maps a cluster.</td>
</tr>
<tr>
<td>Server belongs to cluster</td>
<td>Cluster to which the server belongs. &lt;br&gt;<strong>NOTE:</strong> The properties <strong>Server is cluster</strong> and <strong>Server belongs to cluster</strong> are mutually exclusive.</td>
</tr>
<tr>
<td>IP address (IPv6)</td>
<td>Internet protocol version 6 (IPv6) server address.</td>
</tr>
<tr>
<td>IP address (IPv4)</td>
<td>Internet protocol version 4 (IPv4) server address.</td>
</tr>
<tr>
<td>Copy process (source server)</td>
<td>Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the Robocopy and rsync programs are supported.</td>
</tr>
<tr>
<td></td>
<td>If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed with the Robocopy program between servers with a Windows operating system or with the rsync program between servers with a Linux operating system. If the operating systems of the source and destination servers differ, it is important that the right copy method is applied for successful replication. A copy method is chosen that supports both servers.</td>
</tr>
<tr>
<td>Copy process (target server)</td>
<td>Permitted copying methods that can be used when this server is the destination of a copy action.</td>
</tr>
<tr>
<td>Coding</td>
<td>Character set coding that is used to write files to the server.</td>
</tr>
<tr>
<td>Parent Job server</td>
<td>Name of the parent Job server.</td>
</tr>
<tr>
<td>Executing server</td>
<td>Name of the executing server. The name of the server that exists physically and where the processes are handled.</td>
</tr>
<tr>
<td></td>
<td>This input is evaluated when One Identity Manager Service is automatically updated. If the server is handling several queues the process steps are not...</td>
</tr>
<tr>
<td>Property</td>
<td>Meaning</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>supplied until all the queues that are being processed on the same server have completed their automatic update.</td>
</tr>
<tr>
<td>Queue</td>
<td>Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.</td>
</tr>
<tr>
<td>Server operating system</td>
<td>Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values <strong>Win32, Windows, Linux</strong> and <strong>Unix</strong> are permitted. If no value is specified, <strong>Win32</strong> is used.</td>
</tr>
<tr>
<td>Service account data</td>
<td>One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server) the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain and the service account password have to be entered for the server.</td>
</tr>
<tr>
<td>One Identity Manager Service installed</td>
<td>Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the procedure <strong>QBM_JJobQueueLoad</strong> the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.</td>
</tr>
<tr>
<td>Stop One Identity Manager Service</td>
<td>Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the program &quot;Job Queue Info&quot;. For more detailed information, see the <strong>One Identity Manager Process Monitoring and Troubleshooting Guide</strong>.</td>
</tr>
<tr>
<td>No automatic software update</td>
<td>Specifies whether to exclude the server from automatic software updating. <strong>NOTE:</strong> Servers must be manually updated if this option is set.</td>
</tr>
<tr>
<td>Software update running</td>
<td>Specifies whether a software update is currently being executed.</td>
</tr>
<tr>
<td>Server function</td>
<td>Server functionality in One Identity Manager. One Identity Manager processes are handled depending on the server function.</td>
</tr>
</tbody>
</table>

**Related topics**

- [Specifying server functions](#) on page 98
### Specifying server functions

**NOTE:** All editing options are also available in Designer under **Base Data | Installation | Job server.**

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled depending on the server function.

**NOTE:** More server functions may be available depending on which modules are installed.

#### Table 40: Permitted server functions

<table>
<thead>
<tr>
<th>Server function</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSV connector</td>
<td>Server on which the CSV connector for synchronization is installed.</td>
</tr>
<tr>
<td>Domain controller</td>
<td>The Active Directory domain controller. Servers that are not labeled as domain controller are considered to be member servers.</td>
</tr>
<tr>
<td>Printer server</td>
<td>Server which acts as a print server.</td>
</tr>
<tr>
<td>Generic server</td>
<td>Server for generic synchronization with a custom target system.</td>
</tr>
<tr>
<td>Home server</td>
<td>Server for adding home directories for user accounts.</td>
</tr>
<tr>
<td>Update Server</td>
<td>This server executes automatic software updating of all other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. The server can execute SQL tasks. The server with the installed One Identity Manager database, is labeled with this functionality during initial installation of the schema.</td>
</tr>
<tr>
<td>SQL processing server</td>
<td>The server can execute SQL tasks. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.</td>
</tr>
<tr>
<td>CSV script server</td>
<td>The server can process CSV files using the ScriptComponent process component.</td>
</tr>
<tr>
<td>Native database connector</td>
<td>The server can connect to an ADO.Net database.</td>
</tr>
<tr>
<td>One Identity Manager database connector</td>
<td>Server on which the One Identity Manager connector is installed. This server executes synchronization with the target system One Identity Manager.</td>
</tr>
<tr>
<td>One Identity</td>
<td>Server on which a One Identity Manager Service is installed.</td>
</tr>
<tr>
<td><strong>Server function</strong></td>
<td><strong>Remark</strong></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Manager Service installed</td>
<td></td>
</tr>
<tr>
<td>Primary domain controller</td>
<td>Primary domain controller.</td>
</tr>
<tr>
<td>Profile server</td>
<td>Server for setting up profile directories for user accounts.</td>
</tr>
<tr>
<td>SAM synchronization Server</td>
<td>Server for running synchronization with an SMB-based target system.</td>
</tr>
<tr>
<td>SAP R/3 connector</td>
<td>Server on which the SAP R/3 connector is installed. This server executes synchronization with the target system SAP R/3.</td>
</tr>
<tr>
<td>SMTP host</td>
<td>Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.</td>
</tr>
<tr>
<td>Default report server</td>
<td>Server on which reports are generated.</td>
</tr>
<tr>
<td>Windows PowerShell connector</td>
<td>The server can run Windows PowerShell version 3.0 or later.</td>
</tr>
</tbody>
</table>

**Related topics**

- [Master data for a Job server](#) on page 95

**Target system managers**

A default application role exists for the target system manager in One Identity Manager. Assign the employees who are authorized to edit all clients in One Identity Manager to this application role.

Define additional application roles if you want to limit the edit permissions for target system managers to individual clients. ns for target system managers to individual farms. SharePoint The application roles must be added under the default application role.

For detailed information about implementing and editing application roles, see the [One Identity Manager Authorization and Authentication Guide](#).
Implementing application roles for target system managers

1. The One Identity Manager administrator assigns employees to be target system managers.
2. These target system managers add employees to the default application role for target system managers.
   Target system managers with the default application role are authorized to edit all tenants in One Identity Manager.
3. Target system managers can authorize other employees within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual tenants.

Table 41: Default Application Roles for Target System Managers

<table>
<thead>
<tr>
<th>User</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target system managers</td>
<td>Target system managers must be assigned to **Target systems</td>
</tr>
<tr>
<td></td>
<td>Users with this application role:</td>
</tr>
<tr>
<td></td>
<td>• Assume administrative tasks for the target system.</td>
</tr>
<tr>
<td></td>
<td>• Create, change or delete target system objects, like user accounts or groups.</td>
</tr>
<tr>
<td></td>
<td>• Edit password policies for the target system.</td>
</tr>
<tr>
<td></td>
<td>• Prepare system entitlements for adding to the IT Shop.</td>
</tr>
<tr>
<td></td>
<td>• Can add employees, who have an other identity than the <strong>Primary identity</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager.</td>
</tr>
<tr>
<td></td>
<td>• Edit the synchronization's target system types and outstanding objects.</td>
</tr>
<tr>
<td></td>
<td>• Authorize other employees within their area of responsibility as target system managers and create child application roles if required.</td>
</tr>
</tbody>
</table>

To initially specify employees to be target system administrators

1. Log in to One Identity Manager as Manager administrator (**Base role | Administrators**)
2. Select **One Identity Manager Administration | Target systems | Administrators.**
3. Select **Assign employees.**
4. Assign the employee you want and save the changes.
To add the first employees to the default application as target system managers.

1. Log yourself into Manager as target system administrator (Target systems | Administrators).
2. Select One Identity Manager Administration | Target systems | SAP R/3.
3. Select Assign employees in the task view.
4. Assign the employees you want and save the changes.

To authorize other employees as target system managers when you are a target system manager

1. Login to Manager as target system manager.
2. Select the application role in SAP R/3 | Basic configuration data | Target system managers.
3. Select Assign employees.
4. Assign the employees you want and save the changes.

To specify target system managers for individual clients

1. Log in to Manager as target system manager.
2. Select SAP R/3 | Tenants.
3. Select the tenant in the result list.
4. Select Change master data.
5. On the General tab, select the application role in the Target system manager menu.
   - OR -
   Next to the Target system manager menu, click to create a new application role.
   a. Enter the application role name and assign the Target systems | SAP R/3 parent application role.
   b. Click OK to add the new application role.
6. Save the changes.
7. Assign employees to this application role who are permitted to edit the client in One Identity Manager.

Related topics

- One Identity Manager users for managing an SAP R/3 environment on page 11
- General master data for an SAP client on page 103
NOTE: The Synchronization Editor sets up SAP systems in the One Identity Manager database.

To edit an SAP system's master data

1. Select SAP R/3 | Systems.
2. Select an SAP system in the result list and run Change master data.
3. Edit the system's master data.
4. Save the changes.

Table 42: Master data for an SAP system

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>The SAP system's display name.</td>
</tr>
<tr>
<td>System number</td>
<td>The SAP system number.</td>
</tr>
<tr>
<td>System measurement</td>
<td>Specifies whether system measurement for this system is carried out.</td>
</tr>
<tr>
<td>measurement enabled</td>
<td>One Identity Manager provides the measurement data but the actual system</td>
</tr>
<tr>
<td></td>
<td>measurement takes place in the SAP R/3 environment.</td>
</tr>
</tbody>
</table>

Related topics

- Providing system measurement data on page 182
SAP clients

**NOTE:** One Identity Manager sets up the clients in the Synchronization Editor database.

**To edit client master data**

1. Select the category **SAP R/3 | Tenants**.
2. Select the client in the result list. Select **Change master data**.
3. Edit the client’s master data.
4. Save the changes.

**General master data for an SAP client**

Enter the following general data on **General**.

**Table 43: General master data for a client**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client no.</td>
<td>Number of the client.</td>
</tr>
<tr>
<td>Name</td>
<td>Client's name.</td>
</tr>
<tr>
<td>System</td>
<td>System to which the client belongs.</td>
</tr>
<tr>
<td>Canonical name</td>
<td>Client's canonical name.</td>
</tr>
<tr>
<td>Company</td>
<td>Company for which the client is set up. The company given here is used when a new user account is set up.</td>
</tr>
<tr>
<td>City</td>
<td>City where company resides.</td>
</tr>
<tr>
<td>Has user administration</td>
<td>Specifies whether the client is used for user administration.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Account definition (initial)</td>
<td>Initial account definition for creating user accounts. This account definition is used if automatic assignment of employees to user accounts is used for this client and if user accounts are to be created that are already managed (Linked configured). The account definition's default manage level is applied. User accounts are only linked to the employee (Linked) if no account definition is given. This is the case on initial synchronization, for example.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If the CUA status Child is assigned, no account definition should be assigned.</td>
</tr>
<tr>
<td>Target system managers</td>
<td>Application role in which target system managers are specified for the client. Target system managers only edit objects from the client assigned to them. Each client can have a different target system manager assigned to it. Select the One Identity Manager application role whose members are responsible for administration of this client. Use the button to add a new application role.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You can only specify the synchronization type when adding a new client. No changes can be made after saving. When you create system using the Synchronization Editor, One Identity Manager is used. Type of synchronization through which data is synchronized between the client and One Identity Manager. As soon as objects for this client are available in One Identity Manager, the type of synchronization can no longer be changed. Use One Identity Manager when you create a client with the Synchronization Editor.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you select No synchronization, you can define custom processes to exchange data between One Identity Manager and the target system.</td>
</tr>
<tr>
<td></td>
<td><strong>Table 44: Permitted values</strong></td>
</tr>
<tr>
<td>Value</td>
<td>Synchronization by</td>
</tr>
<tr>
<td>One Identity Manager</td>
<td>SAP R/3 connector</td>
</tr>
<tr>
<td>No synchronization</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you select No synchronization, you can define custom processes to exchange data between One Identity Manager and the target system.</td>
</tr>
</tbody>
</table>
| ALE name                             | Name used to map the client as logical system in the SAP distribution}
### Property Description

- **ALE model name**: Name of the SAP distribution model that maps the relation between the logical systems of the central user administration. SAP roles and profiles of all child systems with the same ALE model name as the central system, are synchronized when the central system is synchronized.

- **CUA status**: Client usage when the central user administration is in use. Possible values are **Central** and **Child**. The value **None** indicates that the client is not being used in a central user administration.

- **CUA central system**: Central system to which the client belongs. Assign the relevant system for clients with the CUA status **Child**.

- **Description**: Spare text box for additional explanation.

### Related topics

- Setting up account definitions on page 58
- Assigning account definitions to a target system on page 73
- Target system managers on page 99
- Special features of synchronizing with a CUA central system on page 32
- Excluding a child system from synchronization on page 33

### Specifying categories for inheriting SAP groups, SAP roles and SAP profiles

**NOTE:** In order to easy understanding the behavior is described with respect to SAP groups in this section. It applies in the same way to roles and profiles.

In One Identity Manager, groups can be selectively inherited by user accounts. For this purpose, the groups and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the other tables enter your categories for the target system-dependent groups. Each table contains the category positions **Position 1** to **Position 31**.

**NOTE:** If central user administration is implemented, define the categories in the central system as well as in the child system. The same categories must be defined in the child system as in the central system so that groups from a child system can be inherited by user accounts.
To define a category

1. In Manager, select the tenant in SAP R/3 | Tenants.
2. Select Change master data.
3. Switch to the Mapping rule category tab.
4. Extend the relevant roots of a table.
5. Click ☑️ to enable category.
6. Enter a category name of your choice for user accounts and groups and in the login language used.
7. Save the changes.

Detailed information about this topic

- Inheriting SAP groups, SAP roles, and SAP profiles based on categories on page 164
- One Identity Manager Target System Base Module Administration Guide

Editing a synchronization project

Synchronization projects in which a client is already used as a base object can also be opened in Manager. You can, for example, check the configuration or view the synchronization log in this mode. The Synchronization Editor is not started with its full functionality. You cannot run certain functions, such as, running synchronization or simulation, starting the target system browser and others.

**NOTE:** Manager is locked for editing throughout. To edit objects in Manager, close the Synchronization Editor.

To open an existing synchronization project in the Synchronization Editor

1. Select SAP R/3 | Tenants.
2. Select the client in the result list. Select Change master data.
3. Select Edit synchronization project... from the task view.

Detailed information about this topic

- One Identity Manager Target System Synchronization Reference Guide

Related topics

- Customizing synchronization configuration on page 35
SAP user accounts

You can manage the users of a One Identity Manager environment with the SAP R/3. One Identity Manager concentrates on setting up and editing SAP user accounts. Groups, roles and profiles are mapped in SAP, in order to provide the necessary permissions for One Identity Manager user accounts. The necessary data for system measurement is also mapped. The system measurement data is available in One Identity Manager, but the measurement itself takes place in the SAP R/3 environment.

If user accounts are managed through the central user administration (CUA) in SAP R/3, access to the child client can be guaranteed to or withdrawn from user accounts in One Identity Manager.

**Detailed information about this topic**

- Linking user accounts to employees on page 107
- Supported user account types on page 108
- Entering SAP user account master data on page 114

**Linking user accounts to employees**

The central component of the One Identity Manager is to map employees and their master data with permissions through which they have control over different target systems. For this purpose, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to employees. This gives an overview of the permissions for each employees in all of the connected target systems. One Identity Manager provides the possibility to manage user accounts and their permissions. You can provision modifications in the target systems. Employees are supplied with the necessary permissions in the connected target systems according to their function in the company. Regular synchronization keeps data consistent between target systems and the One Identity Manager database.

Because requirements vary between companies, the One Identity Manager offers different methods for supplying user accounts to employees. One Identity Manager supports the following method for linking employees and their user accounts.
Employees can automatically obtain their account definitions using user account resources. If an employee does not yet have a user account in a client, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism and subsequent process handling. When you manage account definitions through user accounts, you can specify the way user accounts behave when employees are enabled or deleted.

When user accounts are inserted, they can be automatically assigned to an existing employee or a new employee can be created if necessary. In the process, the employee master data is created on the basis of existing user account master data. This mechanism can be implemented if a new user account is created manually or by synchronization. However, this is not the One Identity Manager default method. Define criteria for finding employees for automatic employee assignment.

Employees and user accounts can be entered manually and assigned to each other.

Related topics

- Entering SAP user account master data on page 114
- Setting up account definitions on page 58
- Automatic assignment of employees to SAP user accounts on page 132

For more detailed information about employee handling and administration, see the One Identity Manager Target System Base Module Administration Guide.

**Supported user account types**

Different types of user accounts, such as default user accounts, administrative user accounts, service accounts, or privileged user accounts can be mapped in One Identity Manager.

The following properties are used for mapping different user account types.

- Identity

  The **Identity** property (IdentityType column) is used to describe the type of user account.

<table>
<thead>
<tr>
<th>Table 45: Identities of user accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>Primary identity</td>
</tr>
<tr>
<td>Identity</td>
</tr>
<tr>
<td>----------------------</td>
</tr>
<tr>
<td>Organizational identity</td>
</tr>
<tr>
<td>Personalized admin identity</td>
</tr>
<tr>
<td>Sponsored identity</td>
</tr>
<tr>
<td>Shared identity</td>
</tr>
<tr>
<td>Service identity</td>
</tr>
</tbody>
</table>

**NOTE:** To enable working with identities for user accounts, the employees also need identities. You can only link user accounts to which an identity is assigned with employees who have this same identity.

The primary identity, the organizational identity, and the personal admin identity are used for different user accounts, which can be used by the same actual employee to execute their different tasks within the company.

To provide user accounts with a personal admin identity or an organizational identity for an employee, you create subidentities for the employee. These subidentities are then linked to user accounts, enabling you to assign the required Entitlements to the different user accounts.

User accounts with a sponsored identity, group identity, or service identity are linked to dummy employees that do not refer to a real person. These dummy employees are needed so that Entitlements can be inherited by the user accounts. When evaluating reports, attestations, or compliance checks, check whether dummy employees need to be considered separately.

For detailed information about mapping employee identities, see the One Identity Manager Identity Management Base Module Administration Guide.

- Privileged user account

  Privileged user accounts are used to provide employees with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are marked as **Privileged user account** (Column IsPrivilegedAccount).

### Default User Accounts

Normally, each employee obtains a default user account, which has the permissions they require for their regular work. The user accounts are linked to the employee. The effect of
the link and the scope of the employee’s inherited properties on the user accounts can be configured through an account definition and its manage levels.

To create default user accounts through account definitions

1. Create an account definition and assign the Unmanaged and Full managed manage levels.
2. Specify the effect of temporarily or permanently disabling, deleting or the security risk of an employee on its user accounts and group memberships for each manage level.
3. Create a formatting rule for IT operating data.
   You use the mapping rule to define which rules are used to map the IT operating data for the user accounts, and which default values are used if no IT operating data can be determined via a person's primary roles.
   Which IT operating data is required depends on the target system. The following setting are recommended for default user accounts:
   - In the mapping rule for the IsGroupAccount column, use the default value 1 and enable Always use default value.
   - In the mapping rule for the IdentityType column, use the default value Primary and enable Always use default value.
4. Enter the effective IT operating data for the target system. Select the concrete target system under Effects on.
   Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.
5. Assign the account definition to employees.
   When the account definition is assigned to an employee, a new user account is created through the inheritance mechanism and subsequent processing.

Administrative User Accounts

An administrative user account must be used for certain administrative tasks. Administrative user accounts are usually predefined by the target system and have fixed names and login names, such as Administrator.

Administrative user accounts are imported into One Identity Manager during synchronization.

| NOTE: | Some administrative user accounts can be automatically identified as privileged user accounts. To do this, enable the Mark selected user accounts as privileged schedule in Designer. |

You can label administrative user accounts as a Personalized administrator identity or as a Shared identity. Proceed as follows to provide the employees who use this user account with the required permissions.
Personalized admin identity

1. Use the UID_Person column to link the user account with an employee.
   Use an employee with the same identity or create a new employee.
2. Assign this employee to hierarchical roles.

Shared identity

1. Assign all employees with usage authorization to the user account.
2. Link the user account to a dummy employee using the UID_Person column.
   Use an employee with the same identity or create a new employee.
3. Assign this dummy employee to hierarchical roles.

The dummy employee provides the user account with its permissions.

Privileged User Accounts

Privileged user accounts are used to provide employees with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are marked as **Privileged user account** (Column IsPrivilegedAccount).

**NOTE:** The criteria according to which user accounts are automatically identified as privileged are defined as extensions to the view definition (ViewAddOn) in the TSBVAccountIsPrivDetectedRule table (which is a table of the **Union** type). The evaluation is done in the script TSB_SetIsPrivilegedAccount.

To create privileged users through account definitions

1. Create an account definition. Create a new manage level for privileged user accounts and assign this manage level to the account definition.
2. If you want to prevent the properties for privileged user accounts from being overwritten, set the **IT operating data overwrites** property for the manage level to **Only initially**. In this case, the properties are populated just once when the user accounts is created.
3. Specify the effect of temporarily or permanently disabling or deleting, or the security risk of an employee on its user accounts and group memberships for each manage level.
4. Create a formatting rule for IT operating data.
   You use the mapping rule to define which rules are used to map the IT operating data for the user accounts, and which default values are used if no IT operating data can be determined via a person’s primary roles.
   Which IT operating data is required depends on the target system. The following settings are recommended for privileged user accounts:
   - In the mapping rule for the IsPrivilegedAccount column, use the default value **1** and enable **Always use default value**.
   - You can also specify a mapping rule for the IdentityType column. The column owns different permitted values that represent user accounts.
• To prevent privileged user accounts from inheriting the entitlements of the default user, define a mapping rule for the IsGroupAccount column with a default value of 0 and enable **Always use default value**.

5. Enter the effective IT operating data for the target system.
   
   Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.

6. Assign the account definition directly to employees who work with privileged user accounts.

   When the account definition is assigned to an employee, a new user account is created through the inheritance mechanism and subsequent processing.

   **TIP:** If customization requires that the login names of privileged user accounts follow a defined naming convention, create the template according to which the login names are formed.

---

**Central user administration in One Identity Manager**

If user accounts are managed through the central user administration (CUA) in SAP R/3, access to the child client can be guaranteed to or withdrawn from user accounts in One Identity Manager. To do this, clients are marked as central system or child system in One Identity Manager. User accounts are managed in the central system. You specify the client in which each user account obtains its access permissions. (SAPUserMandant table). Only SAP groups, role or profiles from these clients can be assigned to a user account. A user account only has access authorizations in the central system if the central system is also explicitly assigned in the SAPUserMandant table.

To use automatic employee assignment for central user administration (CUA) user accounts, assign and account definition to the CUA central system using the **SAPUser** user table.

The access authorizations for central and child systems are read into the One Identity Manager database through synchronization. In One Identity Manager, access authorization can be granted by IT Shop requests and indirect assignment, as well as by indirect assignment.

**To grant a person access to a client by indirect assignment or request**

1. Create an account definition to generate user accounts in the central system.

   In the **User account table** input field, select the **SAPUser** table. For more information, see **Master data for an account definition** on page 59.

   This account definition is required to generate a user account in the central system if the employee does not yet have a user account.

2. Create an account definition for the client for which you want to grant access. The
following special features apply:

**Table 46: Master data of an account definition for accessing clients**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User account table</td>
<td>Select <strong>SAPUserMandant</strong> from the menu.</td>
</tr>
<tr>
<td>Target system</td>
<td>Client for which you want to grant access.</td>
</tr>
<tr>
<td>Required account definition</td>
<td>From the menu, select the account definition to generate user accounts in the central system. A user account is then created in the central system if the employee does not yet have a user account.</td>
</tr>
<tr>
<td>Manage level (initial)</td>
<td>Select <strong>Unmanaged</strong> from the menu.</td>
</tr>
<tr>
<td>Service item</td>
<td>Service item through which you can request the account definition in the IT Shop. Assign an existing service item or add a new one.</td>
</tr>
<tr>
<td>IT Shop</td>
<td>Enable the option if access to the child system can be requested in the Web Portal.</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>Enable the option if access to the child system can only be requested in the Web Portal. Indirect assignment by business roles or organizations is not possible. However, access by a user account to the child system can still be granted directly.</td>
</tr>
</tbody>
</table>

An account definition is required for each child system and for the central system in which you want to grant access.

3. Assign the account definition for the client to a hierarchical role or IT Shop shelf.
4. Add the person as a member to the hierarchical role or as a customer to the IT Shop.

**To grant a user account direct access to a client**

- Assign all the clients to the user account to which it can have access permissions.
  
  For more information, see [Granting access to clients of a central user administration](on page 129).

You can now assign the SAP groups, roles, and profiles from this client to the user account.

**Detailed information about this topic**

- [Setting up account definitions](on page 58)
Related topics

- General master data for an SAP client on page 103
- Assigning SAP groups, SAP roles, and SAP profiles to SAP user accounts on page 148
- Automatic assignment of employees to SAP user accounts on page 132

Entering SAP user account master data

A user account can be linked to an employee in One Identity Manager. You can also manage user accounts separately from employees.

NOTE: It is recommended to use account definitions to set up user accounts for company employees. In this case, some of the master data described in the following is mapped through templates from employee master data.

NOTE: If employees are to obtain their user accounts through account definitions, the employees must own a central SAP user account and obtain their IT operating data through assignment to a primary department, a primary location or a primary cost center.

To create a user account

1. In Manager, select SAP R/3 | User accounts.
2. Click in the result list.
3. On the master data form, edit the master data for the user account.
4. Save the changes.

To edit master data for a user account

1. In Manager, select SAP R/3 | User accounts.
2. Select the user account in the result list and run Change master data.
3. Edit the user account's resource data.
4. Save the changes.

To manually assign or create a user account for an employee

1. Select the Employees | Employees.
2. Select the employee in the result list and run Assign SAP user accounts from the task view.
3. Assign a user account.
4. Save the changes.
Detailed information about this topic

- General master data of an SAP user account on page 115
- SAP user account login data on page 119
- Telephone numbers on page 120
- Fax numbers on page 121
- Email addresses on page 122
- Assigning parameters on page 124
- Fixed values for an SAP user account on page 123
- Measurement data on page 124
- SNC data for an SAP user account on page 125

General master data of an SAP user account

Table 47: Configuration parameters for risk assessment of SAP user accounts

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER\CalculateRiskIndex</td>
<td>Preprocessor relevant configuration parameter controlling system components for calculating an employee’s risk index. Changes to the parameter require recompiling the database.</td>
</tr>
<tr>
<td></td>
<td>If the parameter is enabled, values for the risk index can be entered and calculated.</td>
</tr>
</tbody>
</table>

NOTE: You can only add user account to client which are marked as central system if user accounts in the SAP system managed with central user administration.

Enter general data for a user account on the Address tab.

Table 48: SAP user account address data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. If you are using automatic employee assignment, an associated employee is found and added to the user account when you save the user account. For a user account with an identity of type Organizational identity, Personalized administrator identity, Sponsored identity, Shared identity or Service identity, you can create a new...</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Account definition</td>
<td>Account definition through which the user account was created. Use the account definition to automatically fill user account master data and to specify a manage level for the user account. The One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account.</td>
</tr>
<tr>
<td>Manage level</td>
<td>Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.</td>
</tr>
<tr>
<td>Client</td>
<td>The client to be added in the user account. Central system, if user accounts are manged with CUA. You can only edit the client when the user account is added.</td>
</tr>
<tr>
<td>User account</td>
<td>User account identifier If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>First name</td>
<td>User’s first name If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Last name</td>
<td>Last name of user account If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.</td>
</tr>
<tr>
<td>Form of address</td>
<td>Form of address in the associated client’s language. If you have assigned an account definition, the form of address is found by template rule depending on the manage level. The form of address depends on the gender of the assigned employee.</td>
</tr>
<tr>
<td>Academic title</td>
<td>Additional information about the user account.</td>
</tr>
<tr>
<td>Alias</td>
<td>Alternative ID for the user account that is used as log in for certain internet transactions.</td>
</tr>
<tr>
<td>Nickname</td>
<td>Additional information about the user account.</td>
</tr>
</tbody>
</table>
| Name formatting        | Name format and country for name formatting. Name and country formats determine the formatting rules for composing a full name of an employee in SAP R/3. Name formatting specifies the order in which parts of names are put together so that an employee’s name is repres-
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country for name formatting</td>
<td>The country serves to uniquely identify the formatting rule.</td>
</tr>
<tr>
<td>ISO 639 - language</td>
<td>Default language for the user account according to ISO 639</td>
</tr>
<tr>
<td>Function</td>
<td>Additional information about the user account. Used when addresses are printed.</td>
</tr>
<tr>
<td>Employee number</td>
<td>SAP internal key for identifying an employee.</td>
</tr>
<tr>
<td>Department</td>
<td>Additional information about the user account. Used when addresses are printed.</td>
</tr>
<tr>
<td>Room in building</td>
<td>Additional information about the user account.</td>
</tr>
<tr>
<td>Floor</td>
<td>Additional information about the user account.</td>
</tr>
<tr>
<td>Building (number or token)</td>
<td>Additional information about the user account.</td>
</tr>
<tr>
<td>Communications type</td>
<td>Unique identifier for the communications type</td>
</tr>
<tr>
<td>Company</td>
<td>The company to which the user account is assigned. When a user account is added, the company of the assigned client is used. If the client is not assigned to a company, the company with the smallest address number is found and assigned to the user account.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Company is a required field. Changes to user accounts cannot be saved in SAP R/3 on synchronization if a company is not assigned to them in One Identity Manager. Assign a default company to these user accounts in the SAP R/3 system where possible.</td>
</tr>
<tr>
<td>Risk index (calculated)</td>
<td>Maximum risk index value of all assigned groups, roles and profiles. The property is only visible if the QER</td>
</tr>
<tr>
<td>Category</td>
<td>Categories for the inheritance of groups, roles, and profiles by the user account. To do this, groups, roles, and profiles and user accounts or contacts are divided into categories. Select one or more categories from the menu.</td>
</tr>
</tbody>
</table>
### Property | Description
--- | ---
Identity | User account's identity type Permitted values are:
  - **Primary identity**: Employee's default user account.
  - **Organizational identity**: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.
  - **Personalized administrator identity**: User account with administrative entitlements, used by one employee.
  - **Sponsored identity**: User account that is used for training purposes, for example.
  - **Shared identity**: User account with administrative entitlements, used by several employees. Assign all employees show use the user account.
  - **Service identity**: Service account.

Privileged user account | Specifies whether this is a privileged user account.
Groups can be inherited | Specifies whether the user account can inherit groups, roles and profiles via the employee. If this option is set, the user account inherits groups, roles and profiles via hierarchical roles or IT Shop requests.
  - If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups.
  - If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.

### Related topics
- Linking user accounts to employees on page 107
- Supported user account types on page 108
- Setting up account definitions on page 58
- Specifying categories for inheriting SAP groups, SAP roles and SAP profiles on page 105
- General master data for an SAP client on page 103
- One Identity Manager Identity Management Base Module Administration Guide
- One Identity Manager Target System Base Module Administration Guide
- One Identity Manager Risk Assessment Administration Guide
SAP user account login data

When a user is added, you issue them with a password. Once you have saved the user account password with the Manager it cannot be changed.

Enter the following data on the Login data tab.

Table 49: SAP user account login data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Password for the user account. The employee’s central password can be mapped to the user account password. For detailed information about an employee’s central password, see One Identity Manager Identity Management Base Module Administration Guide. If you use an initial password for the user accounts, it is automatically entered when a user account is created.</td>
</tr>
<tr>
<td>Password confirmation</td>
<td>Reconfirm password.</td>
</tr>
<tr>
<td>Set effective password</td>
<td>Specifies whether the password status &quot;Active password&quot; is set if it is changed in the target system.</td>
</tr>
<tr>
<td>Disabled password</td>
<td>Specifies whether the password is disabled (if single sign-on is used for logging in).</td>
</tr>
<tr>
<td>Security policy</td>
<td>Security policy for this user account.</td>
</tr>
<tr>
<td>User group</td>
<td>SAP group to use as user group for checking permissions.</td>
</tr>
<tr>
<td>Reference user</td>
<td>The user account contains authorizations for this reference user. A reference user is user account with the user type &quot;Reference&quot;. Use reference users to supply identical authorizations to different user accounts within one client.</td>
</tr>
<tr>
<td>Account is valid from</td>
<td>Validity period of the SAP user account.</td>
</tr>
<tr>
<td>Account is valid until</td>
<td></td>
</tr>
<tr>
<td>Accounting number</td>
<td>Number for user account’s accounting.</td>
</tr>
<tr>
<td>Cost center</td>
<td>Cost center for the user account’s accounting.</td>
</tr>
</tbody>
</table>

NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements.

NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User account type</td>
<td>Type of user account. The default user account type is specified in the configuration parameter &quot;TargetSystem\SAPR3\Accounts\Ustyp&quot;.</td>
</tr>
<tr>
<td>User account locked</td>
<td>Specifies whether the user account is locked.</td>
</tr>
<tr>
<td>Last login</td>
<td>Date and time of last target SAP system login.</td>
</tr>
</tbody>
</table>

**Related topics**

- Password policies for SAP user accounts on page 81
- Initial password for new SAP user accounts on page 91
- Email notifications about login data on page 93
- User account types on page 76
- SAP Locking user accounts on page 131
- Security policies on page 79

**Telephone numbers**

You can edit user account email addresses in **Phone numbers**.

**To assign a phone number to a user account**

1. Select **Phone numbers**.
2. Click **Add**.
   
   This inserts a new row in the table.
3. Mark this row. Edit the telephone number master data.
4. Save the changes.

**To edit a phone number**

1. Select **Phone numbers**.
2. Select the phone number in the list.
3. Edit the telephone number master data.
4. Save the changes.

**To remove a phone number assignment**

1. Select **Phone numbers**.
2. Select the phone number in the list.
3. Click **Delete**.
4. Save the changes.

### Table 50: Phone number properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of phone connection Select either &quot;Phone&quot;, &quot;Phone (default)&quot;, &quot;Mobile (default)&quot; or &quot;Mobile&quot;.</td>
</tr>
<tr>
<td>Country</td>
<td>Country for determining the country code.</td>
</tr>
<tr>
<td>Phone</td>
<td>Phone number with local code. Enter an extension number in the extra field. If you have assigned an account definition, the telephone number is found by template rule depending on the manage level.</td>
</tr>
<tr>
<td>Phone number (complete)</td>
<td>Full phone number. Contains dialing code, connection and extension numbers.</td>
</tr>
<tr>
<td>Default number</td>
<td>Specifies whether this phone number is the user's default number.</td>
</tr>
<tr>
<td>Home address</td>
<td>Specifies whether this phone number is the user's home number.</td>
</tr>
<tr>
<td>SMS-enabled</td>
<td>Specifies whether text messages can be sent through this phone number.</td>
</tr>
</tbody>
</table>

**Fax numbers**

You can edit user account email addresses in **Fax numbers**.

### To assign a fax number to a user account

1. Select **Fax numbers**.
2. Click **Add**.
   - This inserts a new row in the table.
3. Mark this row. Edit the fax number master data.
4. Save the changes.

### To edit a fax number

1. Select **Fax numbers**.
2. Select the fax number in the list.
3. Edit the fax number master data.
4. Save the changes.
To remove a fax number assignment

1. Select Fax numbers.
2. Select the fax number in the list.
3. Click Delete.
4. Save the changes.

Table 51: Fax numbers

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>Country for determining the country code.</td>
</tr>
<tr>
<td>Fax number</td>
<td>Fax number with local area code. Enter an extension number in the extra field.</td>
</tr>
<tr>
<td>Fax number (complete)</td>
<td>Full fax number. Contains dialing code, connection and extension numbers.</td>
</tr>
<tr>
<td>Default number</td>
<td>Specifies whether this fax number is the user's default number.</td>
</tr>
<tr>
<td>Home address</td>
<td>Specifies whether this fax number is the user's home number.</td>
</tr>
</tbody>
</table>

Email addresses

You can edit user account email addresses in Email addresses.

To assign an email address to a user account

1. Select Email addresses.
2. Click Add.
   This inserts a new row in the table.
3. Mark this row. Edit the email address master data.
4. Save the changes.

To edit an email address

1. Select Email addresses.
2. Select the email address in the list.
3. Edit the email address master data.
4. Save the changes.

To remove an email address assignment

1. Select Email addresses.
2. Select the email address in the list.
3. Click **Delete**.
4. Save the changes.

### Table 52: Email address data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email address (SMTP)</td>
<td>Email address.</td>
</tr>
<tr>
<td>Email address search</td>
<td>Contains the first 20 characters of the email address in normalized form.</td>
</tr>
<tr>
<td>Default address</td>
<td>Specifies whether this email address is the user's default address.</td>
</tr>
<tr>
<td>Home address</td>
<td>Specifies whether this email address is the user's home address.</td>
</tr>
</tbody>
</table>

### Fixed values for an SAP user account

#### Table 53: Configuration parameters for setting up user accounts

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetSystem\SAPR3\Accounts\Datfm</td>
<td>Specifies the default date format for SAP user accounts.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Dcpfm</td>
<td>Specifies the default decimal point format for SAP user accounts.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Fax_Group</td>
<td>Specifies the default fax group for SAP user accounts.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Guiflag</td>
<td>Specifies whether secure communication is permitted for SAP user accounts.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Spda</td>
<td>Specifies default setting for printer parameter 3 (delete after print).</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Spdb</td>
<td>Specifies default setting for printer parameter 3 (print immediately).</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Splg</td>
<td>Specifies the default printer (print parameter 1).</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Time_zone</td>
<td>Specifies the default time zone value for the SAP user account’s address.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Tzone</td>
<td>Specifies the default value for the time zone.</td>
</tr>
</tbody>
</table>

Enter the default values that are to be put into effect for the user account in **Fixed values**. This includes data such as the start menu, which should be shown after login, the default
login language, personal time zone, decimal representation or date format that the user is going to work with.

To specify default values for fixed values

- Set the configuration parameter values under "TargetSystem\SAPR3\Accounts" in Designer.

Measurement data

The license data for system measurement is shown in Measurement data. For more information, see Providing system measurement data on page 182.

Assigning parameters

You can assign a user account parameter on the Parameter tab and specify its values.

To assign a parameter to a user account

1. Select Parameter.
2. Click Add.
   This inserts a new row in the table.
3. Mark this row. Select a parameter from the Parameter list and specify a parameter value.
4. Save the changes.

To edit a parameter value

1. Select Parameter.
2. Select the parameter whose value you want to edit, in the list.
3. Change the parameter value.
4. Save the changes.

To remove a parameter assignment

1. Select Parameter.
2. Select the parameter you want to remove.
3. Click Delete.
4. Save the changes.
**SNC data for an SAP user account**

Enter the data required for logging into the system over secure network communications (SNC) on the SNC tab.

<table>
<thead>
<tr>
<th>Table 54: User account SNC data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Properties</strong></td>
</tr>
<tr>
<td>SNC Name</td>
</tr>
<tr>
<td>Insecure communication allowed</td>
</tr>
</tbody>
</table>

**Additional tasks for managing SAP user accounts**

After you have entered the master data, you can run the following tasks.

**Overview of the SAP user account**

*To obtain an overview of a user account*

1. Select SAP R/3 | User accounts.
2. Select the user account in the result list.
3. Select SAP user account overview.

**Changing the manage level of an SAP user account**

The default manage level is applied if you create user accounts using automatic employee assignment. You can change a user account manage level later.

*To change the manage level for a user account*

1. In Manager, select SAP R/3 | User accounts.
2. Select the user account in the result list.
3. Select **Change master data**.
4. On the **Address** tab, select the manage level in the **Manage level** menu.
5. Save the changes.

**Related topics**
- General master data of an SAP user account on page 115

### Assigning SAP groups and SAP profiles directly to an SAP user account

Groups and profiles can be assigned directly or indirectly to a user account. Indirect assignment is carried out by allocating the employee, groups and profiles in hierarchical roles, like departments, cost centers, locations or business roles. If the employee has an SAP user account, the groups and profiles in the role are inherited by the user account.

To react quickly to special requests, you can assign groups and profiles directly to the user account.

**NOTE:**
- Only profiles that are not assigned to SAP roles can be assigned to user accounts.
- Generated profiles cannot be assigned to user accounts.
- If the user account is managed through a CUA, groups, and profiles can be selected from all clients assigned to this user account.

**To assign groups and profiles directly to user accounts**

1. Select **SAP R/3 | User accounts**.
2. Select the user account in the result list.
3. Select one of the following tasks.
   - **Assign groups**, to assign SAP groups directly.
   - **Assign profiles**, to assign SAP profiles directly.
4. Assign groups or profiles in **Add assignments**.
   - **OR** -
   - In **Remove assignments**, delete the groups or profiles.
5. Save the changes.

**Related topics**
- Assigning SAP groups, SAP roles, and SAP profiles to SAP user accounts on page 148
Assigning SAP roles directly to an SAP user account

Roles can be assigned directly or indirectly to a user account. Indirect assignment is carried out by allocating the employee and roles in hierarchical roles, like departments, cost centers, locations or business roles. If the employee has an SAP user account, the SAP roles in the hierarchical roles are inherited by the user account.

To react quickly to special requests, you can assign roles directly to the user account.

If the user account is managed through a CUA, roles can be selected from all clients assigned to this user account.

**To assign roles directly to user accounts**

1. Select SAP R/3 | User accounts.
2. Select the user account in the result list.
3. Select Assign roles.

**To assign a role**

1. Click Add.
   
   This inserts a new row in the table.
2. Select the role you want to assign from Role.
3. Enter a validity period for the role assignment in Valid from and Valid until, if that applies.
4. Assign more roles as necessary.
5. Save the changes.

**To edit a role assignment**

1. Select the role assignment you want to edit in the table. Edit the validity period.
2. Save the changes.

**To remove a role assignment.**

1. Select the role assignment you want to remove in the table.
2. Click Delete.
3. Save the changes.

**Related topics**

- Assigning SAP user accounts directly to SAP roles on page 153
Assigning structural profiles

Installed modules:  SAP R/3 Structural Profiles Add-on Module

Structural profiles can be assigned directly or indirectly to a user account. Indirect assignment is carried out by allocating the employee and structural profiles in hierarchical roles, like departments, cost centers, locations or business roles. If the employee has an SAP user account, the structural profiles in the role are inherited by the user account. To react quickly to special requests, you can assign structural profiles directly to the user account.

To assign structural profiles directly to user accounts
1. Select SAP R/3 | User accounts.
2. Select the user account in the result list.
3. Select Assign structural profiles.

To assign a structural profile
1. Click Add.
   This inserts a new row in the table.
2. Select the structural profile to assign from Structural profile.
3. Enter a validity period for the profile assignment in Valid from and Valid until, if it applies.
4. Assign more structural profiles as necessary.
5. Save the changes.

To edit a profile assignment
1. Select the profile assignment you want to edit in the table. Edit the validity period.
2. Save the changes.

To remove a profile assignment
1. Select the profile assignment you want to remove in the table.
2. Click Delete.
3. Save the changes.

Detailed information about this topic
- One Identity Manager Administration Guide for SAP R/3 Structural Profiles Add-on
Granting access to clients of a central user administration

User accounts, administered through central user administration (CUA), have control over access permissions in several clients. You specify the client in which each user account obtains its access permissions. Clients can be assigned directly and indirectly. For indirect assignments, create account definitions for the clients and assign these to hierarchical roles. For more information, see Central user administration in One Identity Manager on page 112.

To react quickly to special requests, you can assign the clients directly to a user account. You can select the central system and the child system in this process. Only SAP groups, role or profiles from these clients can be assigned to a user account. This task is only available if the client of the selected user account is labeled as central system.

To assign a user account directly to a client

1. Select SAP R/3 | User accounts.
2. Select the user account in the result list.
3. Select Assign access to clients.

To assign a client

1. Click Add.
   This inserts a new row in the table.
2. From the Client menu, select the client in which you want the user account to receive access permissions.
3. Assign an account definition, if necessary.
4. Assign more clients, if necessary.
5. Save the changes.

To edit an assignment

1. In the table, select the assignment that you want to edit. Edit the account definition’s assignment.
2. Save the changes.

To remove an assignment

1. In the table, select the assignment that you want to remove.
2. Click Delete.
3. Save the changes.
SAP Licenses assign

**NOTE:** This task is only available for user account managed through CUA.

SAP licenses in child system and in the central system can be assigned to user account for system measurement. For more information, see Providing system measurement data on page 182.

**To assign licenses to a user account**

1. Select the SAP R/3 | User accounts category.
2. Select the user account in the result list.
3. Select SAP Assign licenses in client systems.
4. Click Add.
   - This inserts a new row in the table.
5. Mark this row. Enter the measurement data.
6. Save the changes.

**To edit a license assignment**

1. Select the SAP R/3 | User accounts category.
2. Select the user account in the result list.
3. Select SAP Assign licenses in client systems.
4. Select an assignment in the table.
5. Edit the measurement data.
6. Save the changes.

**To remove a license assignment**

1. Select the SAP R/3 | User accounts category.
2. Select the user account in the result list.
3. Select SAP Assign licenses in client systems.
4. Select an assignment in the table.
5. Click Delete.
6. Save the changes.

The following license information is displayed on the form.

**Table 55: Measurement Data for a Centrally administrated User Account**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipient</td>
<td>Client containing the user account which is assigned a license. You can</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>client</td>
<td>select the central system or a assigned child system.</td>
</tr>
<tr>
<td>License</td>
<td>User account license in the selected client.</td>
</tr>
<tr>
<td>License extension</td>
<td>License extension for the installed special version. Select the special</td>
</tr>
<tr>
<td></td>
<td>version ID from the menu.</td>
</tr>
<tr>
<td>Country</td>
<td>surcharge</td>
</tr>
<tr>
<td></td>
<td>Additional license fee.</td>
</tr>
<tr>
<td>Chargeable</td>
<td>system</td>
</tr>
<tr>
<td></td>
<td>SAP system containing the client to be charged. This field is only shown if</td>
</tr>
<tr>
<td></td>
<td>&quot;04 (substitute)&quot; or &quot;11 (Multi-client/system)&quot; is entered.</td>
</tr>
<tr>
<td>Chargeable</td>
<td>client</td>
</tr>
<tr>
<td></td>
<td>Client containing the user account to be charged. This field is only shown if</td>
</tr>
<tr>
<td></td>
<td>&quot;04 (substitute)&quot; or &quot;11 (Multi-client/system)&quot; is entered.</td>
</tr>
<tr>
<td>Chargeable</td>
<td>user account</td>
</tr>
<tr>
<td></td>
<td>User account to be charged if &quot;04 (substitute)&quot; or &quot;11 (Multi-client/sys-</td>
</tr>
<tr>
<td></td>
<td>tem)&quot; is entered.</td>
</tr>
<tr>
<td>Substituted</td>
<td>from</td>
</tr>
<tr>
<td></td>
<td>Time period in which another user account assumes responsibility. This</td>
</tr>
<tr>
<td></td>
<td>input field is enabled if the active license is set to &quot;04 (substitute)&quot;.</td>
</tr>
<tr>
<td>Substituted</td>
<td>until</td>
</tr>
</tbody>
</table>

**Related topics**

- Special versions on page 81

**SAP Locking user accounts**

The way that user accounts are managed determines how you lock them. User accounts that are not linked to an employee, can be locked with **Lock user account**.

**To lock a user account**

1. Select **SAP R/3 | User accounts**.
2. Select the user account in the result list.
3. Select **Lock user account** from the task view.
4. Confirm the prompt with **OK**.

   This generates a process that publishes the change in the target system. The **User account locked** option is enabled as soon as the process is successfully completed.

**To unlock a user account**

1. Select **SAP R/3 | User accounts**.
2. Select the SAP user account in the result list.
3. Select **Unlock user account** from the task view.
4. Confirm the prompt with **OK**.
   
   This generates a process that publishes the change in the target system. The **User account locked** option is disabled as soon as the process is successfully completed.

**Detailed information about this topic**
- Locking SAP user accounts on page 137

## Assigning extended properties

Extended properties are meta objects that cannot be mapped directly in One Identity Manager, for example, operating codes, cost codes or cost accounting areas.

**To specify extended properties for a user account**

1. Select **SAP R/3 | User accounts**.
2. Select the user account in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.
   - OR -
   
   Remove extended properties from **Remove assignments**.
5. Save the changes.

**Detailed information about this topic**
- One Identity Manager Identity Management Base Module Administration Guide

## Automatic assignment of employees to SAP user accounts

**Table 56: Configuration parameters for automatic employee assignment**

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetSystem\SAPR3\PersonAutoFullSync</td>
<td>This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.</td>
</tr>
<tr>
<td>Configuration parameter</td>
<td>Meaning</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\PersonAutoDefault</td>
<td>This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.</td>
</tr>
</tbody>
</table>
| TargetSystem\SAPR3\PersonExcludeList | List of all user accounts for which automatic employee assignment should not take place. Names are listed in a pipe (|) delimited list that is handled as a regular search pattern. 
Example: SAP*|SAPCPIC|SAPJSF|DDIC|J2EE_ADMIN|J2EE_GUEST |
| TargetSystem\SAPR3\PersonAutoDisabledAccounts | This configuration parameter specifies whether employees are automatically assigned to disable user accounts. User accounts do not obtain an account definition. |

When you add a user account, an existing employee can be assigned automatically or added if necessary. In the process, the employee master data is created on the basis of existing user account master data. This mechanism can follow on after a new user account has been created manually or through synchronization. Define criteria for finding employees to apply to automatic employee assignment. If a user account is linked to an employee through the current mode, the user account is given, through an internal process, the default manage level of the account definition entered in the user account’s target system. You can customize user account properties depending on how the behavior of the manage level is defined.

If you run this procedure during working hours, automatic assignment of employees to user accounts takes place from that moment onwards. If you disable the procedure again later, the changes only affect user accounts added or updated after this point in time. Existing employee assignment to user accounts remain intact.

**NOTE:** It is not recommended to assign employees using automatic employee assignment in the case of administrative user accounts. Use **Change master data** to assign employees to administrative user account for the respective user account.

Run the following tasks to assign employees automatically.

- If employees can be assigned by user accounts during synchronization, set "TargetSystem\SAPR3\PersonAutoFullsync" in the Designer and select the mode.
- If employees can be assigned by user accounts during synchronization, set "TargetSystem\SAPR3\PersonAutoDefault" in the Designer and select the mode.
Specify the user accounts in "TargetSystem\SAPR3\PersonExcludeList", which must not be assigned automatically to employees.

Example:
SAP*|SAPCPIC|SAPJSF|DDIC|J2EE_ADMIN|J2EE_GUEST

Use the configuration parameter 
"TargetSystem\SAPR3\PersonAutoDisabledAccounts" to specify whether employees can be automatically assigned to disabled user accounts. User accounts do not obtain an account definition.

Assign an account definition to the client. Ensure that the manage level to be used is entered as the default manage level.

Define the search criteria for employee assignment in the client.

NOTE:
The following applies for synchronization:

- Automatic employee assignment takes effect if user accounts are added or updated.

The following applies outside synchronization:

- Automatic employee assignment takes effect if user accounts are added.

NOTE:
Following a synchronization, employees are automatically created for the user accounts in the default installation. If an account definition for the client is not yet known at the time of synchronization, user accounts are linked with employees. However, account definitions are not assigned. The user accounts are therefore in a Linked state.

To manage the user accounts using account definitions, assign an account definition and a manage level to these user accounts.

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the client.
3. Assign the account definition and manage level to user accounts in linked status.
   a. In Manager, select SAP R/3 | User accounts | Linked but not configured | <Client>.
   b. Select Assign account definition to linked accounts.

Detailed information about this topic

- One Identity Manager Target System Base Module Administration Guide
Related topics

- Creating an account definition on page 59
- Assigning account definitions to a target system on page 73
- Editing the search criteria for automatic employee assignment on page 135

Editing the search criteria for automatic employee assignment

The criteria for employee assignment are defined for the client. In this case, you specify which user account properties must match the employee’s properties such that the employee can be assigned to the user account. You can limit search criteria further by using format definitions. The search criterion is written in XML notation to the **Search criteria for automatic employee assignment** column (AccountToPersonMatchingRule) in the SAPMandant table.

Search criteria are evaluated when employees are automatically assigned to user accounts. Furthermore, you can create a suggestion list for assignments of employees to user accounts based on the search criteria and make the assignment directly.

**NOTE:** When the employees are assigned to user accounts on the basis of search criteria, user accounts are given the default manage level of the account definition entered in the user account’s target system. You can customize user account properties depending on how the behavior of the manage level is defined.

It is not recommended to make assignment to administrative user accounts based on search criteria. Use **Change master data** to assign employees to administrative user account for the respective user account.

**NOTE:** One Identity Manager supplies a default mapping for employee assignment. Only carry out the following steps when you want to customize the default mapping.

To specify criteria for employee assignment

1. Select **SAP R/3 | Clients**.
2. Select the client in the result list.
3. Select **Define search criteria for employee assignment** in the task view.
4. Specify which user account properties must match with which employee so that the
employee is linked to the user account.

**Table 57: Standard search criteria for user accounts**

<table>
<thead>
<tr>
<th>Apply to</th>
<th>Column for employee</th>
<th>Column for user account</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP user accounts of the type &quot;Dialog&quot;</td>
<td>Central SAP user account</td>
<td>User account</td>
</tr>
<tr>
<td></td>
<td>(CentralSAPAccount)</td>
<td>(Accnt)</td>
</tr>
</tbody>
</table>

5. Save the changes.

**Direct assignment of employees to user accounts based on a suggestion list**

In Assignments, you can create a suggestion list for assignments of employees to user accounts based on the search criteria and make the assignment directly. User accounts are grouped in different views for this.

**Table 58: Manual Assignment View**

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suggested assignments</td>
<td>This view lists all user accounts to which One Identity Manager can assign an employee. All employees are shown who were found using the search criteria and can be assigned.</td>
</tr>
<tr>
<td>Assigned user accounts</td>
<td>This view lists all user accounts to which an employee is assigned.</td>
</tr>
<tr>
<td>Without employee assignment</td>
<td>This view lists all user accounts to which no employee is assigned and for which no employee was found using the search criteria.</td>
</tr>
</tbody>
</table>

**TIP:** By double-clicking on an entry in the view, you can view the user account and employee master data.

**To apply search criteria to user accounts**

- Click **Reload**.
  
  All possible assignments based on the search criteria are found in the target system for all user accounts. The three views are updated.

**To assign employees directly over a suggestion list**

1. Click **Suggested assignments**.
   
   a. Click **Select** for all user accounts to which you want to assign the suggested employees. Multi-select is possible.
b. Click Assign selected.

c. Confirm the security prompt with Yes.

The employees determined using the search criteria are assigned to the selected user accounts.

– OR –

2. Click No employee assignment.

a. Click Select employee for the user account to which you want to assign an employee. Select an employee from the menu.

b. Click Select for all user accounts to which you want to assign the selected employees. Multi-select is possible.

c. Click Assign selected.

d. Confirm the security prompt with Yes.

The employees displayed in the Employee column are assigned to the selected user accounts.

To remove assignments

1. Click Assigned user accounts.

a. Click Select for all user accounts for which you want to delete the employee assignment. Multi-select is possible.

b. Click Remove selected.

c. Confirm the security prompt with Yes.

The assigned employees are removed from the selected user accounts.

For detailed information about defining search criteria, see the One Identity Manager Target System Base Module Administration Guide.

Related topics

- Automatic assignment of employees to SAP user accounts on page 132

Locking SAP user accounts

The way you lock user accounts depends on how they are managed.

Scenario:

- The user account is linked to employees and is managed through account definitions.

User accounts managed through account definitions are locked when the employee is temporarily or permanently disabled. The behavior depends on the user account manage level. Accounts with the manage level Full managed manage level are disabled depending on the account definition settings. The Lock user account and Unlock user account...
tasks cannot be applied to these accounts. For user accounts with a manage level, configure the required behavior using the template in the SAPUser.U_Flag

Scenario:

- The user accounts are linked to employees. No account definition is applied.

User accounts managed through user account definitions are locked when the employee is temporarily or permanently disabled. The behavior depends on the QER | Person | TemporaryDeactivation configuration parameter

- If the configuration parameter is set, the employee’s user accounts are locked if the employee is permanently or temporarily disabled. The Lock user account and Unlock user account tasks cannot be applied to these accounts.
- If the configuration parameter is not set, the employee’s properties do not have any effect on the associated user accounts.

To lock the user account when the configuration parameter is disabled.

1. In Manager, select SAP R/3 | User accounts.
2. Select the user account in the result list.
3. Select Lock user account from the task view.
4. Confirm the prompt with OK.

Scenario:

- User accounts not linked to employees.

To lock a user account that is no longer linked to an employee.

1. In Manager, select SAP R/3 | User accounts.
2. Select the user account in the result list.
3. Select Lock user account from the task view.
4. Confirm the prompt with OK.

A process is generated, which publishes this user account modification in the target system. Once the lock has been published in the target system, User account locked is enabled on Login data. The user can no longer log in with this user account.

To unlock a user account

1. Select SAP R/3 | User accounts.
2. Select the user account in the result list.
3. Select Unlock user account from the task view.
4. Confirm the prompt with OK.

This generates a process that publishes the change in the target system. The option User account locked is disabled as soon as the process is successfully completed.
Detailed information about this topic

For more information, see the One Identity Manager Target System Base Module Administration Guide.

Related topics

- Setting up account definitions on page 58
- Creating manage levels on page 62

Deleting and restoring SAP user accounts

**NOTE:** As long as an account definition for an employee is valid, the employee retains the user account that was created by it. If the assignment of an account definition is removed, the user account that was created from this account definition is deleted.

**To delete a user account**

1. Select **SAP R/3 | User accounts**.
2. Select the user account in the result list.
3. Click to delete the user account.
4. Confirm the security prompt with Yes.

**To restore a user account**

1. Select **SAP R/3 | User accounts**.
2. Select the user account in the result list.
3. Click in the result list toolbar.

Configuring deferred deletion

By default, user accounts are finally deleted from the database after 30 days. The user accounts are initially disabled. You can reenable the user accounts until deferred deletion is run. After deferred deletion is run, the user account are deleted from the database and cannot be restored anymore. You can configure an alternative deletion delay on the table SAPUser in Designer. Deferred deletion has no influence over the login permission in assigned CUA child systems.
Entering external user identifiers for an SAP user account

External authentication methods for logging on to a system can be used in SAP R/3. With One Identity Manager, you can maintain login data for logging in external system users, for example, Active Directory on an SAP R/3 environment.

You can use One Identity Manager to enter external user IDs and delete them. You can only change the option “Account is enabled” for existing user ID’s.

To enter external IDs

1. Select SAP R/3 | External IDs.
2. Select the external identifier in the result list. Select Change master data.
   - OR -
   Click in the result list.
3. Enter the required data on the master data form.
4. Save the changes.

Enter the following data for an external identifier.

Table 59: External ID properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External user ID</td>
<td>User login name for the user to log into external systems. The syntax you require depends on the type of authentication selected. The complete user identifier is compiled by template.</td>
</tr>
</tbody>
</table>

**NOTE:** The BAPI One Identity Manager uses the default settings RSUSREXT for generating the user identifier, which means that the user name is reset. The value provided in the interface is passed as prefix.

If you SAP R/3 environment uses something other than these default settings, modify the template for column SAPUserExtId.EXTID respectively.

| External identifier type | Authentication type for the external user. This results in the syntax for the external identifier. |

Table 60: External identifier types

- Distinguished Name for X.509
- Login uses the distinguished name for X.509
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows NTLM or</td>
<td>Login uses Windows NT Lan Manager or password verification with the Windows</td>
</tr>
<tr>
<td>password verification</td>
<td>domain controller.</td>
</tr>
<tr>
<td>LDAP bind &lt;user defined&gt;</td>
<td>Login uses LDAP bind (for other authentication mechanisms).</td>
</tr>
<tr>
<td>SAML token</td>
<td>Authentication uses an SAML token profile.</td>
</tr>
</tbody>
</table>

The default type is specified in "TargetSystem\SAPR3\Accounts\ExtID_Type".

<table>
<thead>
<tr>
<th>Target system type</th>
<th>Can be called up together with the external ID type to test the login data. The default type is specified in &quot;TargetSystem\SAPR3\Accounts\TargetSystemID&quot;. Permitted values are ADSACCOUNT and NTACCOUNT.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account is enabled</td>
<td>Specifies whether the user or an external authentication system can log in to the system.</td>
</tr>
<tr>
<td>User account</td>
<td>Assignment of the external user ID to a user account.</td>
</tr>
<tr>
<td>Sequential number</td>
<td>Sequential number, if a user account has more than one external identifiers.</td>
</tr>
<tr>
<td>Valid from</td>
<td>Date from which the external user ID is valid.</td>
</tr>
</tbody>
</table>

Related topics

- [External identifier types](#) on page 77
SAP groups, SAP roles and SAP profiles

Groups, roles and profiles are mapped in the One Identity Manager, in order to provide the necessary permissions for user accounts. Groups, roles, and profiles can be assigned to user accounts, requested or inherited through hierarchical roles in One Identity Manager. No new groups, roles, or profiles can be added or deleted.

Groups
You can share maintenance of user accounts over different administrators by assigning user accounts to groups.

Roles
A role includes all transactions and user menus that an SAP user requires to fulfill its tasks. Roles are separated into single and collective roles. Single roles can be grouped together into collective roles. User account members in the roles can be set for a limit period.

Profiles
Access permissions to the system are regulated through profiles. Profiles are assigned through single roles or directly to user accounts. Profiles can be grouped into collective profiles.

Editing the master data for SAP groups, SAP roles, and SAP profiles

You can edit the following data about groups, roles, and profiles in One Identity Manager:

- Assigned SAP user accounts
- Usage in the IT Shop
- Risk assessment
Inheritance through roles and inheritance restrictions
License information for system measurement

To edit group master data
1. Select the category SAP R/3 | Groups.
2. Select the group in the result list. Select Change master data.
3. Enter the required data on the master data form.
4. Save the changes.

To edit profile master data
1. Select SAP R/3 | Profiles.
2. Select the profile in the result list. Select Change master data.
3. Enter the required data on the master data form.
4. Save the changes.

To edit role master data
1. Select SAP R/3 | Roles.
2. Select the role in the result list. Select Change master data.
3. Enter the required data on the master data form.
4. Save the changes.

Detailed information about this topic
- General master data for SAP groups on page 143
- General master data for SAP roles on page 145
- General master data for SAP profiles on page 146

General master data for SAP groups

Table 61: Configuration parameters for risk assessment of SAP user accounts

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER\CalculateRiskIndex</td>
<td>Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to the parameter require recompiling the database. If the parameter is enabled, values for the risk index can be entered and calculated.</td>
</tr>
</tbody>
</table>

Edit the following master data for a group.
### Table 62: SAP group master data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Name of the group as displayed in One Identity Manager tools. The group name is taken from the group identifier by default.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of group in the target system.</td>
</tr>
<tr>
<td>Client</td>
<td>Client, in which the group is added.</td>
</tr>
<tr>
<td>Service item</td>
<td>Service item data for requesting the group through the IT Shop.</td>
</tr>
<tr>
<td>Risk index</td>
<td>Value for evaluating the risk of assigning the group to user accounts. Enter a value between 0 and 1. This input field is only visible if the configuration parameter **QER</td>
</tr>
<tr>
<td>Category</td>
<td>Categories for group inheritance. Groups can be selectively inherited by user accounts. To do this, groups and user accounts are divided into categories. Select one or more categories from the menu.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>IT Shop</td>
<td>Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles.</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is no permitted.</td>
</tr>
</tbody>
</table>

### Detailed information about this topic

- Specifying categories for inheriting SAP groups, SAP roles and SAP profiles on page 105
- One Identity Manager IT Shop Administration Guide
- One Identity Manager Identity Management Base Module Administration Guide
- One Identity Manager Target System Base Module Administration Guide
- One Identity Manager Risk Assessment Administration Guide
General master data for SAP roles

Table 63: Configuration parameters for risk assessment of SAP user accounts

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER\CalculateRiskIndex</td>
<td>Preprocessor relevant configuration parameter controlling system components for calculating an employee’s risk index. Changes to the parameter require recompiling the database. If the parameter is enabled, values for the risk index can be entered and calculated.</td>
</tr>
</tbody>
</table>

Edit the following master data for a role.

Table 64: SAP role master data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Name of the role as displayed in One Identity Manager tools. Taken from the role identifier by default.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of role in the target system.</td>
</tr>
<tr>
<td>Client</td>
<td>Client, in which the role is added.</td>
</tr>
<tr>
<td>License</td>
<td>Role license. This task is needed for finding system measurement for user accounts and is assigned once after synchronization.</td>
</tr>
<tr>
<td>Role type</td>
<td>Role type for differentiating between single and collective roles.</td>
</tr>
<tr>
<td>Service item</td>
<td>Service item data for requesting the role through the IT Shop.</td>
</tr>
<tr>
<td>Risk index</td>
<td>Value for evaluating the risk of assigning the role to user accounts. Enter a value between 0 and 1. This property is only visible if the configuration parameter &quot;QER\CalculateRiskIndex&quot; is set.</td>
</tr>
<tr>
<td>Category</td>
<td>Categories for role inheritance. User accounts can inherit roles selectively. To do this, roles and user accounts are divided into categories. Use this menu to allocate one or more categories to the role.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Role description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>IT Shop</td>
<td>Specifies whether the role can be requested through the IT Shop. This role can be requested by staff through the Web Portal and granted through a defined approval procedure. The role can still be assigned directly to employees and hierarchical roles.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>Specifies whether the role can only be requested through the IT Shop. This role can be requested by staff through the Web Portal and granted through a defined approval procedure. The role may not assigned directly to hierarchical roles.</td>
</tr>
</tbody>
</table>

**Detailed information about this topic**

- [Licenses](#) on page 80
- [Providing system measurement data](#) on page 182
- [Specifying categories for inheriting SAP groups, SAP roles and SAP profiles](#) on page 105
- One Identity Manager IT Shop Administration Guide
- One Identity Manager Identity Management Base Module Administration Guide
- One Identity Manager Target System Base Module Administration Guide
- One Identity Manager Risk Assessment Administration Guide

**General master data for SAP profiles**

**Table 65: Configuration parameters for risk assessment of SAP user accounts**

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER\CalculateRiskIndex</td>
<td>Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to the parameter require recompiling the database. If the parameter is enabled, values for the risk index can be entered and calculated.</td>
</tr>
</tbody>
</table>

Edit the following master data for a profile.

**Table 66: SAP profile master data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Name of the profile as displayed in One Identity Manager tools. The profile name is taken from the profile identifier by default.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of profile in the target system.</td>
</tr>
<tr>
<td>Client</td>
<td>Client, in which the profile is added.</td>
</tr>
<tr>
<td>License</td>
<td>Profile license. This task is needed for finding system measurement for SAP</td>
</tr>
</tbody>
</table>
## Property

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile type</td>
<td>Profile type for differentiating between single, collective and generated profiles.</td>
</tr>
<tr>
<td>Service item</td>
<td>Service item data for requesting the profile through the IT Shop.</td>
</tr>
<tr>
<td>Risk index</td>
<td>Value for evaluating the risk of assigning the profile to account accounts. Enter a value between 0 and 1. This property is only visible if the configuration parameter &quot;QER\CalculateRiskIndex&quot; is set.</td>
</tr>
<tr>
<td>Category</td>
<td>Category for profile inheritance. User accounts can selectively inherit profiles. To do this, profiles and user accounts are divided into categories. Use this menu to allocate one or more categories to the profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Profile is enabled</td>
<td>Specifies whether the profile is enabled or a maintenance version.</td>
</tr>
<tr>
<td>Limited assignment</td>
<td>Specifies whether the profile is assigned to an SAP role. The profile then no longer be directly assigned to user accounts, business roles, organizations or IT Shop shelves.</td>
</tr>
<tr>
<td>IT Shop</td>
<td>Specifies whether the profile can be requested through the IT Shop. This profile can be requested by staff through the Web Portal and granted through a defined approval procedure. The profile can still be assigned directly to hierarchical roles. This option cannot be enabled for generated profiles.</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>Specifies whether the profile can only be requested through the IT Shop. This profile can be requested by staff through the Web Portal and granted through a defined approval procedure. The profile may not assigned directly to hierarchical roles. This option cannot be enabled for generated profiles.</td>
</tr>
</tbody>
</table>

## Detailed information about this topic

- [Licenses](#) on page 80
- [Providing system measurement data](#) on page 182
- [Specifying categories for inheriting SAP groups, SAP roles and SAP profiles](#) on page 105
- One Identity Manager IT Shop Administration Guide
- One Identity Manager Identity Management Base Module Administration Guide
- One Identity Manager Target System Base Module Administration Guide
- One Identity Manager Risk Assessment Administration Guide
Assigning SAP groups, SAP roles, and SAP profiles to SAP user accounts

Groups, roles and profiles can be directly and indirectly assigned to user accounts. In the case of indirect assignment, employees, groups, roles, and profiles are arranged in hierarchical roles. The number of groups, roles, and profiles assigned to an employee is calculated from the position in the hierarchy and the direction of inheritance. If you add an employee to roles and that employee owns a user account, the user account is added to the group, role, or profile. Prerequisites for indirect assignment of employees to user accounts:

- Assignment of employees and groups, roles, and profiles is permitted for role classes (department, cost center, location, or business role).
- User accounts are marked with the Groups can be inherited option.
- User accounts and groups, roles, and profiles belong to the same SAP clients.

Furthermore, groups, roles, and profiles can be assigned to employees through IT Shop requests. Add employees to a shop as customers so that groups, roles, and profiles can be assigned through IT Shop requests. All groups, roles, and profiles are assigned to this shop can be requested by the customers. Requested groups, roles, and profiles are assigned to the employees after approval is granted.

**NOTE:** Only profiles that are not assigned to an SAP role can be assigned to hierarchical roles.

Detailed information about this topic

- Assigning SAP groups, SAP roles, and SAP profiles to organizations on page 148
- Assigning SAP groups, SAP roles, and SAP profiles to business roles on page 150
- Assigning SAP user accounts directly to SAP groups, and SAP profiles on page 152
- Adding SAP groups, SAP roles, and SAP profiles in system roles on page 154
- Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 156
- Assigning and passing on SAP profiles and SAP roles to SAP user accounts on page 160
- One Identity Manager Identity Management Base Module Administration Guide

Assigning SAP groups, SAP roles, and SAP profiles to organizations

Assign groups, roles, and profiles to departments, cost centers, and locations in order to assign user accounts to them through these organizations.
To assign a group to departments, cost centers or locations (non role-based login)

1. Select SAP R/3 | Groups.
2. Select the group in the result list.
3. Select Assign organizations.
4. Assign organizations in Add assignments.
   - Assign departments on the Departments tab.
   - Assign locations on the Locations tab.
   - Assign cost centers on the Cost centers tab.
   - OR -
     Remove the organizations in Remove assignments.
5. Save the changes.

To assign a role to departments, cost centers, or locations (non-role-based login)

1. Select SAP R/3 | Roles.
2. Select the role in the result list.
3. Select Assign organizations.
4. Assign organizations in Add assignments.
   - Assign departments on the Departments tab.
   - Assign locations on the Locations tab.
   - Assign cost centers on the Cost centers tab.
   - OR -
     Remove the organizations in Remove assignments.
5. Save the changes.

To assign a profile to departments, cost centers, or locations (non-role-based login)

1. Select SAP R/3 | Profiles.
2. Select a profile in the result list.
3. Select Assign organizations.
4. Assign organizations in Add assignments.
   - Assign departments on the Departments tab.
   - Assign locations on the Locations tab.
   - Assign cost centers on the Cost centers tab.
   - OR -
     Remove the organizations in Remove assignments.
5. Save the changes.

To assign groups, roles or profiles to departments, cost centers or locations (non role-based login)

1. Select Organizations | Departments.
   - OR -
   Select the category Organizations | Cost centers.
   - OR -
   Select the category Organizations | Locations.
2. Select the department, cost center or location in the result list.
3. Select Assign SAP groups.
   - OR -
   Select Assign SAP roles.
   - OR -
   Select Assign SAP profiles.
4. Select the groups, roles or profiles in Add assignments.
   - OR -
   In Remove assignments, remove the groups, roles, or profiles.
5. Save the changes.

Related topics
- Assigning SAP groups, SAP roles, and SAP profiles to business roles on page 150
- Assigning SAP user accounts directly to SAP groups, and SAP profiles on page 152
- Adding SAP groups, SAP roles, and SAP profiles in system roles on page 154
- Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 156
- One Identity Manager users for managing an SAP R/3 environment on page 11

Assigning SAP groups, SAP roles, and SAP profiles to business roles

Installed modules: Business Roles Module

You assign groups, roles and profiles to business roles in order to assign them to user accounts over business roles.
To assign a group to a business role (non role-based login)

1. Select SAP R/3 | Groups.
2. Select the group in the result list.
3. Select Assign business roles in the task view.
4. Assign business roles in Add assignments.
   - OR -
   Remove the business roles in Remove assignments.
5. Save the changes.

To assign a role to a business role (non role-based login)

1. Select SAP R/3 | Roles.
2. Select the role in the result list.
3. Select Assign business roles in the task view.
4. Assign business roles in Add assignments.
   - OR -
   Remove the business roles in Remove assignments.
5. Save the changes.

To assign a profile to a business role (non role-based login)

1. Select SAP R/3 | Profiles.
2. Select a profile in the result list.
3. Select Assign business roles in the task view.
4. Assign business roles in Add assignments.
   - OR -
   Remove the business roles in Remove assignments.
5. Save the changes.

To assign groups, roles or profiles to a business role (non role-based login)

1. Select the category Business roles | <Role class>.
2. Select the business role in the result list.
3. Select Assign SAP groups.
   - OR -
   Select Assign SAP roles.
   - OR -
   Select Assign SAP profiles.
4. Select the groups, roles or profiles in Add assignments.
   - OR -
In Remove assignments, remove the groups, roles, or profiles.

5. Save the changes.

Related topics

- Assigning SAP groups, SAP roles, and SAP profiles to organizations on page 148
- Assigning SAP user accounts directly to SAP groups, and SAP profiles on page 152
- Adding SAP groups, SAP roles, and SAP profiles in system roles on page 154
- Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 156
- One Identity Manager users for managing an SAP R/3 environment on page 11

Assigning SAP user accounts directly to SAP groups, and SAP profiles

To react quickly to special requests, you can assign groups and profiles directly to user accounts.

**NOTE:**

- Only profiles that are not assigned to SAP roles can be assigned to user accounts.
- Generated profiles cannot be assigned to user accounts.

The following applies if user accounts are managed by CUA:

- The group (the profile) is assigned to the central system, or
- The group's (the profile's) client is assigned as a child system to the user accounts

To assign a group directly to user accounts

1. Select the category SAP R/3 | Groups.
2. Select the group in the result list.
3. Select Assign user accounts in the task view.
4. Assign user accounts in Add assignments.
   - OR -
   - Remove user accounts from Remove assignments.
5. Save the changes.

To assign a profile directly to user accounts

1. Select SAP R/3 | Profiles.
2. Select a profile in the result list.
3. Select **Assign user accounts** in the task view.
4. Assign user accounts in **Add assignments**.
   - OR -
   Remove user accounts from **Remove assignments**.
5. Save the changes.

**Related topics**
- Assigning SAP groups and SAP profiles directly to an SAP user account on page 126
- Assigning SAP groups, SAP roles, and SAP profiles to organizations on page 148
- Assigning SAP groups, SAP roles, and SAP profiles to business roles on page 150
- Adding SAP groups, SAP roles, and SAP profiles in system roles on page 154
- Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 156

**Assigning SAP user accounts directly to SAP roles**

To react quickly to special requests, you can assign roles directly to user accounts.
The following applies if user accounts are managed by CUA:
- The role is assigned to the central system, or
- The role’s client is assigned as a child system to the user accounts.

**To assign a role directly to user accounts**
1. Select **SAP R/3 | Roles**.
2. Select the role in the result list.
3. Select **Assign user accounts** in the task view.

**To assign a role to a user account**
1. Click **Add**.
   This inserts a new row in the table.
2. Select the user account you want to assign to the role from **User account**.
3. Enter a validity period for the role assignment in **Valid from** and **Valid until**, if that applies.
4. Enter another user account if required.
5. Save the changes.
To edit a role assignment

1. Select the role assignment you want to edit in the table. Edit the validity period.
2. Save the changes.

To remove a role assignment.

1. Select the role assignment you want to remove in the table.
2. Click Delete.
3. Save the changes.

Related topics

- Assigning SAP roles directly to an SAP user account on page 127
- Assigning SAP groups, SAP roles, and SAP profiles to organizations on page 148
- Assigning SAP groups, SAP roles, and SAP profiles to business roles on page 150
- Adding SAP groups, SAP roles, and SAP profiles in system roles on page 154
- Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 156

Adding SAP groups, SAP roles, and SAP profiles in system roles

Installed modules: System Roles Module

Groups, roles and profiles can be added to different system roles. When you assign a system role to an employee, the groups, roles, and profiles are inherited by all SAP user accounts that these employees have. System roles that exclusively contain SAP groups, roles, or profiles can be labeled with "SAP product". Groups, roles and profiles can also be added to system roles that are not SAP products.

**NOTE:** Only profiles that are not assigned to an SAP role can be assigned to system roles.

**NOTE:** Groups, roles, and profiles with Only use in IT Shop can only be assigned to system roles that also have this option set. For more detailed information about providing system roles in the IT Shop, see the One Identity Manager System Roles Administration Guide.

To assign a group to system roles

1. Select the category **SAP R/3 | Groups**.
2. Select the group in the result list.
3. Select **Assign system roles**.
4. Assign system roles in Add assignments.

   **TIP:** In the Remove assignments area, you can remove the assignment of system roles.

   **To remove an assignment**
   - Select the system role and double click ✔.

5. Save the changes.

**To assign a role to system roles**
1. Select SAP R/3 | Roles.
2. Select the role in the result list.
3. Select Assign system roles.
4. Assign system roles in Add assignments.

   **TIP:** In the Remove assignments area, you can remove the assignment of system roles.

   **To remove an assignment**
   - Select the system role and double click ✔.

5. Save the changes.

**To assign a profile to system roles**
1. Select SAP R/3 | Profiles.
2. Select a profile in the result list.
3. Select Assign system roles.
4. Assign system roles in Add assignments.

   **TIP:** In the Remove assignments area, you can remove the assignment of system roles.

   **To remove an assignment**
   - Select the system role and double click ✔.

5. Save the changes.

**Detailed information about this topic**
- SAP Products on page 170

**Related topics**
- Assigning SAP groups, SAP roles, and SAP profiles to organizations on page 148
- Assigning SAP groups, SAP roles, and SAP profiles to business roles on page 150
Assigning SAP user accounts directly to SAP groups, and SAP profiles on page 152
Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 156

Adding SAP groups, SAP roles, and SAP profiles to the IT Shop

**NOTE:** Only profiles that are not assigned to SAP roles can be assigned to IT Shop shelves.

When you assign a group, a role, or a profile to a IT Shop shelf, it can be requested by the shop customers. To ensure it can be requested, further prerequisites need to be guaranteed.

- the group, the role, or the profile must be marked with the **IT Shop** option.
- the group, the role or profile must be assigned a service item.

**TIP:** In Web Portal, all products that can be requested are grouped together by service category. To make the group, the role, or profile easier to find in Web Portal, assign a service category to the service item.

- If you only want it to be possible for the group, the role or profile to be assigned to employees through IT Shop requests, the group, the role or the profile must also be labeled with the **Use only in IT Shop** option. Direct assignment to hierarchical roles or user accounts is no longer permitted.

**NOTE:** With role-based login, the IT Shop administrators can assign groups, roles, and profiles to IT Shop shelves. Target system administrators are not authorized to add groups, roles, and profiles to IT Shop.

To add a group, a role, or a profile to IT Shop.

1. In Manager, select **SAP R/3 | Groups** or **SAP R/3 | Roles** or **SAP R/3 | Profiles** (non-role-based login).
   - **OR -**
   
   In Manager, select **Entitlements | SAP Groups** or **Entitlements | SAP Roles** or **Entitlements | SAP Profiles** (role-based login).
2. In the result list, select the group, the role or the profile.
3. Select **Add to IT Shop**.
4. In **Add assignments**, assign the group, the role or profile to the IT Shop shelves.
5. Save the changes.
To remove a group, a role or profile from individual shelves of the IT Shop

1. In Manager, select SAP R/3 | Groups or SAP R/3 | Roles or SAP R/3 | Profiles (non-role-based login).
   - OR -
   In Manager, select Entitlements | SAP Groups or Entitlements | SAP Roles or Entitlements | SAP Profiles (role-based login).
2. In the result list, select the group, the role or the profile.
3. Select Add to IT Shop.
4. In Remove assignments, remove the group, the role or profile from the IT Shop shelves.
5. Save the changes.

To remove a group, a role or profile from all shelves of the IT Shop

1. In Manager, select SAP R/3 | Groups or SAP R/3 | Roles or SAP R/3 | Profiles (non-role-based login).
   - OR -
   In Manager, select Entitlements | SAP Groups or Entitlements | SAP Roles or Entitlements | SAP Profiles (role-based login).
2. In the result list, select the group, the role or the profile.
3. Select Remove from all shelves (IT Shop).
4. Confirm the security prompt with Yes.
5. Click OK.
   The group, the role or profile is removed from all shelves by the One Identity Manager Service. All requests and assignment requests with this group, this role or profile are canceled.

For more detailed information about request from company resources through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Related topics

- General master data for SAP groups on page 143
- Assigning SAP groups, SAP roles, and SAP profiles to organizations on page 148
- Assigning SAP groups, SAP roles, and SAP profiles to business roles on page 150
- Assigning SAP user accounts directly to SAP groups, and SAP profiles on page 152
- Adding SAP groups, SAP roles, and SAP profiles in system roles on page 154
Validity period of role assignments

Table 67: Configuration parameter for handling the validity period of requested SAP roles

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetSystem\SAPR3\ValidDateHandling</td>
<td>Configuration parameter for handling the validity period in SAP user account assignments to SAP roles.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\ValidDateHandling\DoNotUsePWODate</td>
<td>This configuration parameter specifies whether the validity dates from request procedure are copied from SAP user account assignments to SAP roles. If the configuration parameter is set, the &quot;Valid from&quot; and &quot;Valid to&quot; dates from the request procedure are not copied from SAP user account assignments to SAP roles.</td>
</tr>
</tbody>
</table>

Assignment of SAP roles to user accounts can be limited to set periods in your SAP R/3 environment. There are different ways of specifying time limits for role assignments in One Identity Manager.

1. Synchronizing Role Assignments
   The columns "Valid from" and "Valid to" are taken into account in the default mapping. Synchronization writes the validity period of role assignments into the One Identity Manager database.

2. Direct assignment of SAP roles to user accounts in the Manager
   A validity period can be entered for direct assignment of roles to user accounts. "Valid from" and "Valid to" dates are provisioned in the target system.

3. Limited time period requests in the IT Shop
   A validity period for a request can be entered in the IT Shop. An entry in SAPUserInSAPRole only exist between the first and last days of the request's validity period.
   a. Directly requesting an SAP role
      Once the request is approved and the "Valid from" date has been reached, the request recipient's SAP user account inherits the SAP role. The role assignments are automatically canceled and deleted when the validity period expires.
The request's validity period is copied to SAPUserInSAPRole by default. This means that the data is provisioned in the SAP environment.

**To prevent the request's validity date is copied to the role assignment**

- In Designer, set the configuration parameter "TargetSystem\SAPR3\ValidDateHandling\DoNotUsePWODate".

b. Membership request in a hierarchical role (for example, a department)

An SAP role is assigned to the hierarchical role.

Once the request is approved and the "Valid from" date is reached, the employees becomes a member in the hierarchical role. The employee’s SAP user account inherits the SAP role. The membership is automatically canceled and the role assignment deleted when the validity period expires.

c. Request for assignment of an SAP role to a hierarchical role.

Employees with an SAP user account are members of this hierarchical role.

Once the request is approved and the "Valid from" date is reached, the SAP role is assigned to the hierarchical role. The role member’s SAP user accounts inherit the SAP role. The assignment is automatically canceled and the role assignment deleted when the validity period expires.

The request's validity period is copied to SAPUserInSAPRole by default. This means that the data is provisioned in the SAP environment.

**To prevent the request's validity date is copied to the role assignment**

- In Designer, set the configuration parameter "TargetSystem\SAPR3\ValidDateHandling\DoNotUsePWODate".

The table SAPUserInSAPRole contains all role assignments, limited and unlimited. The table HelperSAPUserInSAPRole only contains current valid role assignments. Tables are calculated on a schedule.

**Detailed information about this topic**

- Assigning SAP roles directly to an SAP user account on page 127
- Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 156
- One Identity Manager Web Portal User Guide

**Related topics**

- Assigning SAP groups, SAP roles, and SAP profiles to SAP user accounts on page 148
Assigning and passing on SAP profiles and SAP roles to SAP user accounts

The following SAP sided limitation influence the user account assignment and inheritance of profiles and roles in One Identity Manager.

- Collective profiles can be put together from 0...n profiles or collective profiles. If a user account is assigned an collective profile, the target system only returns the user account membership in the assigned collective profile and not the membership in subprofiles.

- Single roles can put together from 0..n profiles. Only profiles that are not collective profiles can be assigned. Profiles that are assigned to a single role can no longer be assigned to a user account.

- Collective roles can be made up of 0...n single roles. Assignment of profiles or collective profiles to collective roles is not possible.

These limitations result in the following:

In assignment:

- Triggering prevents the assignment of roles which are assigned to single roles, to user accounts, products, roles, and employees.

In inheritance behavior:

- If a user account is assigned a collective role that owns single roles, the single roles are not added to the table SAPUserInSAPGroupTotal.

- If a user account is assigned a single role that owns profiles, the profiles are not added to the table SAPUserInSAPProfile

- If a user account is assigned a single role and this single role is part of a collective role that is also assigned to this user account, the single role is not added to the table SAPUserInSAPRole.

- If a user account is assigned a collective profile with child profiles, the child profiles are not added to the table SAPUserInSAPProfile.

If a user account obtains additional roles or profiles through a reference user, these roles or profiles are only added in SAPUserInSAPRole and SAPUserInSAPProfile for the reference user. When company resources assigned to an employee (table PersonHasObject) are calculated, the roles and profiles inherited by a user account through single roles, collective roles, collective profiles, and reference users are also taken into account.

Additional tasks for managing SAP groups, SAP roles, and SAP profiles

After you have entered the master data, you can run the following tasks.
Overview of SAP groups, SAP roles, and SAP profiles

To obtain an overview of a group
1. Select the category SAP R/3 | Groups.
2. Select the group in the result list.
3. Select SAP group overview.

To obtain an overview of a profile
1. Select SAP R/3 | Profiles.
2. Select a profile in the result list.
3. Select SAP profile overview.

To obtain an overview of a role
1. Select SAP R/3 | Roles.
2. Select the role in the result list.
3. Select SAP role overview.

Effectiveness of SAP groups, SAP roles, and SAP profiles

NOTE: In order to easy understanding the behavior is described with respect to SAP groups in this section. It applies in the same way to roles and profiles.

Table 68: Configuration Parameter for Conditional Inheritance

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preprocessor relevant configuration parameter for controlling effectiveness of group memberships. If the parameter is set, memberships can be reduced on the basis of exclusion definitions. Changes to the parameter require recompiling the database.</td>
<td></td>
</tr>
</tbody>
</table>

When groups are assigned to user accounts an employee may obtain two or more groups, which are not permitted in this combination. To prevent this, you can declare mutually exclusive groups. To do this, you specify which of the two groups should apply to the user accounts if both are assigned.

It is possible to assign an excluded group directly, indirectly or by IT Shop request at any time. One Identity Manager determines whether the assignment is effective.
NOTE:

- You cannot define a pair of mutually exclusive groups. That means, the definition "Group A excludes group B" AND "Group B excludes groups A" is not permitted.
- You must declare each group to be excluded from a group separately. Exclusion definitions cannot be inherited.

The effectiveness of the assignments is mapped in the SAPUserInSAPGrp and BaseTreeHasSAPGrp via the column XIsInEffect.

**Example of the effect of group memberships**

- Group A is defined with permissions for triggering requests in a client A group B is authorized to make payments. A group C is authorized to check invoices.
- Group A is assigned through the department "Marketing", group B through "Finance" and group C through the business role "Control group".

Clara Harris has a user account in this client. She primarily belongs to the department "marketing". The business role "Control group" and the department "Finance" are assigned to her secondarily. Without an exclusion definition, the user account obtains all the permissions of groups A, B and C.

By using suitable controls, you want to prevent an employee from being able to trigger a request and to pay invoices. That means, groups A, B and C are mutually exclusive. An employee that checks invoices may not be able to make invoice payments as well. That means, groups B and C are mutually exclusive.

**Table 69: Specifying excluded groups (table SAPGrpExclusionAADGroupExclusion])**

<table>
<thead>
<tr>
<th>Effective Group</th>
<th>Excluded Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A</td>
<td></td>
</tr>
<tr>
<td>Group B</td>
<td>Group A</td>
</tr>
<tr>
<td>Group C</td>
<td>Group B</td>
</tr>
</tbody>
</table>

**Table 70: Effective Assignments**

<table>
<thead>
<tr>
<th>Employee</th>
<th>Member in Role</th>
<th>Effective Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ben King</td>
<td>Marketing</td>
<td>Group A</td>
</tr>
<tr>
<td>Jan Bloggs</td>
<td>Marketing, finance</td>
<td>Group B</td>
</tr>
<tr>
<td>Clara Harris</td>
<td>Marketing, finance, control group</td>
<td>Group C</td>
</tr>
<tr>
<td>Jenny Basset</td>
<td>Marketing, control group</td>
<td>Group A, Group C</td>
</tr>
</tbody>
</table>
Only the group C assignment is in effect for Clara Harris. It is published in the target system. If Clara Harris leaves the business role "control group" at a later date, group B also takes effect.

The groups A and C are in effect for Jenny Basset because the groups are not defined as mutually exclusive. If this should not be allowed, define further exclusion for group C.

**Table 71: Excluded groups and effective assignments**

<table>
<thead>
<tr>
<th>Employee</th>
<th>Member in Role</th>
<th>Assigned Group</th>
<th>Excluded Group</th>
<th>Effective Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jenny Basset</td>
<td>Marketing</td>
<td>Group A</td>
<td>Group B</td>
<td>Group C</td>
</tr>
<tr>
<td></td>
<td>Control group</td>
<td>Group C</td>
<td>Group A</td>
<td></td>
</tr>
</tbody>
</table>

**Prerequisites**

- The "QER\Structures\Inherit\GroupExclusion" configuration parameter is enabled.
- Mutually exclusive groups, roles and profiles belong to the same client.

**To exclude a group**

1. Select the category **SAP R/3 | Groups**.
2. Select the group in the result list.
3. Select **Exclude groups**.
4. Assign the groups that are mutually exclusive to the selected group in **Add assignments**.
   - OR -
   In **Remove assignments**, remove the groups that are not longer mutually exclusive.
5. Save the changes.

**To exclude roles**

1. Select **SAP R/3 | Roles**.
2. Select the role in the result list.
3. Select **Exclude SAP roles** in the task view.
4. Assign the roles that are mutually exclusive to the selected role in **Add assignments**.
   - OR -
In the **Remove assignments** view, remove the roles that no longer exclude each other.

5. Save the changes.

**To exclude profiles**

1. Select **SAP R/3 | Profiles**.
2. Select a profile in the result list.
3. Select **Exclude roles**.
4. Assign the profiles that are mutually exclusive to the selected profile in **Add assignments**.
   - OR -
   In **Remove assignments**, remove the profiles that are no longer mutually exclusive.

5. Save the changes.

**Inheriting SAP groups, SAP roles, and SAP profiles based on categories**

**NOTE:** In order to easily understand the behavior is described with respect to SAP groups in this section. It applies in the same way to roles and profiles.

In One Identity Manager, groups can be selectively inherited by user accounts. For this purpose, the groups and the user accounts are divided into categories. The categories can be freely selected and specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system-dependent user accounts. In the other tables enter your categories for the target system-dependent groups. Each table contains the category positions **Position 1 to Position 31**.

Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category item matches an assigned group. The group is also inherited by the user account if the group or the user account is not put into categories.

**NOTE:** Inheritance through categories is only taken into account when groups are assigned indirectly through hierarchical roles. Categories are not taken into account when groups are directly assigned to user accounts.
Table 72: Category Examples

<table>
<thead>
<tr>
<th>Category Position</th>
<th>Categories for User Accounts</th>
<th>Categories for Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Default user</td>
<td>Default entitlements</td>
</tr>
<tr>
<td>2</td>
<td>System users</td>
<td>System user entitlements</td>
</tr>
<tr>
<td>3</td>
<td>System administrator</td>
<td>System administrator entitlements</td>
</tr>
</tbody>
</table>

Figure 4: Example of inheriting through categories.

![Diagram showing user and group categorization](image)
To use inheritance through categories

- Define the categories in the client.
  
  **NOTE:** If central user administration is implemented, define the categories in the central system as well as in the child system. The same categories must be defined in the child system as in the central system so that groups from a child system can be inherited by user accounts.

- Assign categories to user accounts through their master data.
- Assign categories to groups, roles, and profiles through their master data.

Related topics

- Specifying categories for inheriting SAP groups, SAP roles and SAP profiles on page 105
- General master data of an SAP user account on page 115
- General master data for SAP groups on page 143
- General master data for SAP roles on page 145
- General master data for SAP profiles on page 146

Assigning extended properties to SAP groups, SAP roles and SAP profiles

Extended properties are meta objects that cannot be mapped directly in One Identity Manager, for example, operating codes, cost codes or cost accounting areas.

To specify extended properties for a group

1. Select the category SAP R/3 | Groups.
2. Select the group in the result list.
3. Select Assign extended properties in the task view.
4. Assign extended properties in Add assignments.
   - OR -
   Remove extended properties from Remove assignments.
5. Save the changes.

To specify extended properties for a role

1. Select SAP R/3 | Roles.
2. Select the role in the result list.
3. Select Assign extended properties in the task view.
4. Assign extended properties in **Add assignments**.
   - OR -
   Remove extended properties from **Remove assignments**.
5. Save the changes.

**To specify extended properties for a profile**

1. Select **SAP R/3 | Profiles**.
2. Select a profile in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.
   - OR -
   Remove extended properties from **Remove assignments**.
5. Save the changes.

**SAP Showing authorizations**

You can view authorization objects and authorizations of SAP roles and profiles in One Identity Manager. All single profiles with their associated authorization objects and fields are displayed in a hierarchical overview.

**To display role authorizations**

1. Select **SAP R/3 | Roles**.
2. Select the role in the result list.
3. Select the task **Show SAP authorizations**.

**To display profile authorizations**

1. Select **SAP R/3 | Profiles**.
2. Select a profile in the result list.
3. Select the task **Show SAP authorizations**.
Calculating the validity date of inherited role assignments

Table 73: Configuration parameters for handling for validity dates from indirectly assigned SAP roles

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetSystem\SAPR3\ValidDateHandling</td>
<td>Configuration parameter for handling the validity period in SAP user account assignments to SAP roles.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\ValidDateHandling\ReuseInheritedDate</td>
<td>This configuration parameter specifies whether the validity date of inherited SAP user account assignments to SAP roles remains intact. The configuration parameter is only relevant in systems that were migrated from a pre 7.0 version. If the configuration parameter is set, the date values &quot;Valid from&quot; and &quot;Valid to&quot; stay the same if SAP user account assignments to roles are inherited.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\ValidDateHandling\ReuseInheritedDate\UseTodayForInheritedValidFrom</td>
<td>This configuration parameter specifies whether the &quot;Valid from&quot; date in inherited SAP user accounts assignments to SAP roles is set to &lt;Today&gt; or to &quot;1900-01-01&quot;.</td>
</tr>
</tbody>
</table>

Validity dates of indirectly assigned SAP roles have been saved in a modified format in the One Identity Manager database since One Identity Manager version 7.0 and later.

Table 74: Default date values for validity dates of indirectly assigned SAP roles (table SAPUserInSAPRole)

<table>
<thead>
<tr>
<th>One Identity Manager version</th>
<th>Valid from (ValidFrom)</th>
<th>Valid until (ValidUntil)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;= 7.0</td>
<td>1/1/1900</td>
<td>12/31/9999</td>
</tr>
<tr>
<td>&lt; 7.0</td>
<td>Date on which the role assignment was created</td>
<td>9998-12-31</td>
</tr>
</tbody>
</table>
Existing validity dates in databases migrated from versions older that 7.0 remain as they are. Once a inheritance is recalculated for a user account, all indirectly assigned SAP roles are saved with new validity dates. These changes are immediately provisioned in SAP. This might result in a heavy load on the connected SAP system.

**To prevent validity dates from adjusting to the new format when recalculating inheritance**

- Set "TargetSystem\SAPR3\ValidDateHandling\ReuseInheritedDate" in Designer.

  **IMPORTANT:** In order to ensure that the validity period is correctly calculated straight after migration, set the configuration parameter with a custom change in the migration package. For detailed information about creating a custom migration package, see One Identity One Identity Manager 7.0.2. Migration Guide to Upgrading Previous Versions of One Identity Manager.

If the configuration parameter is set, the validity dates stays the same for existing indirect role assignments meaning that no provisioning tasks are queued. These assignments are not reworked during synchronization with revision filtering.

The new date values are set for newly added indirect assignments. Therefore, it is not obvious when the assignment is valid in the SAP R/3 environment after provisioning. If this information is required, you can enter the actual date that the role assigned is created in the "Valid from" date.

**To apply the current date as "Valid from" date for new indirect assignments**

- Set "TargetSystem\SAPR3\ValidDateHandling\ReuseInheritedDate\UseTodayForInheritedValidFrom" in the Designer.

  The date the role assignment was created is entered in the "Valid from" date if it is an indirect assignment.

  **IMPORTANT:** Calculating indirect role assignments can become much slower depending on the amount of data to be processed.

  Do not set this configuration parameter if it not absolutely necessary to know how long the role assignment has been valid in the SAP R/3 environment.
SAP Products

Installed modules: System Roles Module

You can define One Identity Manager products as a collection of different groups, roles, or profiles in SAP. SAP products are system roles with the system role type "SAP product". Employees can obtain SAP products directly, inherit them through hierarchical role, or request them in the IT Shop.

The employee’s user account is assigned the groups, roles, and profiles in the SAP product independent of the assignment method. If an SAP product changes by adding or removing a group, role, or a profile in One Identity Manager, user account memberships are changed accordingly.

To edit SAP products

1. Select SAP R/3 | Products.
2. Select an SAP product in the result list.
   - OR –
   Click in the result list.
   This opens the master data form for a system role.
3. Edit the system role's master data.
4. Save the changes.

Detailed information about this topic

- One Identity Manager System Roles Administration Guide
General master data for an SAP product

Table 75: Configuration parameters for risk assessment of SAP user accounts

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER\CalculateRiskIndex</td>
<td>Preprocessor relevant configuration parameter controlling system components for calculating an employee’s risk index. Changes to the parameter require recompiling the database. If the parameter is enabled, values for the risk index can be entered and calculated.</td>
</tr>
</tbody>
</table>

Enter the following data for a system role.

Table 76: System role master data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Name for displaying the system roles in One Identity Manager tools.</td>
</tr>
<tr>
<td>System role</td>
<td>Unique identifier for the system role.</td>
</tr>
<tr>
<td>Internal product name</td>
<td>An additional internal name for the system role.</td>
</tr>
<tr>
<td>System role type</td>
<td>Specifies the type of company resources, which comprise the system role.</td>
</tr>
<tr>
<td>Service item</td>
<td>In order to use a service item within the IT Shop, assign a service item to it or add a new service item. For more information about service items, see the One Identity Manager IT Shop Administration Guide.</td>
</tr>
<tr>
<td>System role manager</td>
<td>Manager responsible for the system role. Assign any new employee. This employee can edit system role master data. They can be used as attestors for system role properties. If the system role can be requested in the IT Shop, the manager will automatically be a member of the application role for product owners assigned the service item.</td>
</tr>
<tr>
<td>Share date</td>
<td>Specify a date for enabling the system role. If the date is in the future, the system role is considered to be disabled. If the date is reached, the system role is enabled. Employees inherit company resources that are assigned to the system role. If the share date is exceeded or no date is entered, the system role is handled as an enabled system role. Company resource inheritance can be handled as an enabled system role. Company resource inheritance can be handled as an enabled system role.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Property</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Controlled</td>
<td>controlled with the <strong>Disabled</strong> option in these cases.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Configure and enable the <strong>Share system roles</strong> schedule in Designer to check the share date. For detailed information about schedules, see the <strong>One Identity Manager Operational Guide</strong>.</td>
</tr>
<tr>
<td>Risk index (calculated)</td>
<td>Maximum risk index values for all company resources. The property is only visible if the **QER</td>
</tr>
<tr>
<td>Comment</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Remarks</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Deactivated</td>
<td>Specifies whether employees and workdesks inherit the company resources contained in the system role. If this option is set, the system role can be assigned to employees, workdesks, hierarchical roles and IT Shop shelves. However they cannot inherit the company resources contained in the system role. The system role cannot be requested in the Web Portal. If this option is not set, company resources assigned to the system role are inherited. If the option is enabled at a later date, existing assignments are removed.</td>
</tr>
<tr>
<td>IT Shop</td>
<td>Specifies whether the system role can be requested through the IT Shop. This system role can be requested by staff through the Web Portal and the request granted by a defined approval procedure. The system role can still be assigned directly to employees and hierarchical roles. For detailed information about IT Shop, see the <strong>One Identity Manager IT Shop Administration Guide</strong>.</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>Specifies whether the system role can only be requested through the IT Shop. This system role can be requested by staff through the Web Portal and the request granted by a defined approval procedure. The system role may not assigned directly to hierarchical roles.</td>
</tr>
<tr>
<td>Spare field no. 01 ...   Spare field no. 10</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
</tbody>
</table>

For detailed information about system roles, see the **One Identity Manager System Roles Administration Guide**
Assigning SAP products to employees

SAP products can be assigned directly or indirectly to employees. In the case of indirect assignment, employees, and SAP products are arranged in hierarchical roles. The number of SAP products assigned to an employee is calculated from the position in the hierarchy and the direction of inheritance.

If you add an employee to roles and that employee owns a user account, the user account is added to all groups, roles, or profiles included in the SAP products owned by the employee. The groups, roles, or profiles are not inherited if the SAP product is disabled or if the share date is still in the future.

Prerequisites for indirect assignment:

- Assignment of system roles, employees, groups, roles, and profiles is permitted for role classes (department, cost center, location, or business role).
- User accounts are marked with the **Groups can be inherited** option.
- The user accounts, groups, roles, and profiles belong to the same SAP client.

Furthermore, IT Shop products can be assigned to employees through SAP requests. SAP products can be assigned through IT Shop requests by adding employees to a shop as customers. All SAP products are assigned to this shop can be requested by the customers. Requested SAP products are assigned to the employees after approval is granted.

**Detailed information about this topic**

- Assigning SAP products to organizations on page 173
- Assigning SAP products to business roles on page 174
- Assigning SAP products directly to employees on page 175
- Adding SAP products in system roles on page 175
- Adding SAP products to the IT Shop on page 176
- One Identity Manager Identity Management Base Module Administration Guide

**Related topics**

- Assigning SAP groups, SAP roles, and SAP profiles to SAP user accounts on page 148

**Assigning SAP products to organizations**

Assign SAP products to departments, cost centers, and locations in order to assign employees to them through these organizations.
To assign an SAP product to departments, cost centers, or locations

1. Select SAP R/3 | Products.
2. Select the SAP product in the result list.
3. Select Assign organizations.
4. Assign organizations in Add assignments.
   - Assign departments on the Departments tab.
   - Assign locations on the Locations tab.
   - Assign cost centers on the Cost centers tab.
   - OR -
     Remove the organizations in Remove assignments.
5. Save the changes.

Related topics
- Assigning SAP products to business roles on page 174
- Adding SAP products to the IT Shop on page 176
- Assigning SAP products directly to employees on page 175
- Adding SAP products in system roles on page 175
- Assigning SAP groups, SAP roles, and SAP profiles to organizations on page 148

Assigning SAP products to business roles

Installed modules: Business Roles Module

You assign SAP products to business roles in order to assign them to user accounts over business roles.

To assign an SAP product to business roles

1. Select SAP R/3 | Products.
2. Select the SAP product in the result list.
3. Select Assign business roles in the task view.
4. Assign business roles in Add assignments.
   - OR -
     Remove the business roles in Remove assignments.
5. Save the changes.
Assigning SAP products directly to employees

You can assign SAP products directly to employees. All groups, roles and profiles are assigned to this SAP product can be inherited by these employees.

To assign an SAP product directly to employees

1. Select SAP R/3 | Products.
2. Select the SAP product in the result list.
3. Select Assign to employees in the task view.
4. Assign employees in Add assignments.
   - OR -
   - Remove employees from Remove assignments.
5. Save the changes.

Related topics

- Assigning SAP products to organizations on page 173
- Assigning SAP products to business roles on page 174
- Adding SAP products to the IT Shop on page 176
- Adding SAP products in system roles on page 175

Adding SAP products in system roles

You can group individual SAP products into a package. To do this, you assign SAP products to system roles.

NOTE: SAP products with Only use in IT Shop set can only be assigned to system roles that also have this option set.
To assign an SAP product to system roles

1. Select SAP R/3 | Products.
2. Select the SAP product in the result list.
3. Select Assign system roles.
4. Select the tab System role contained in to assign parent system roles.
   - Assign system roles in Add assignments.
     - OR -
     Delete the system roles in Remove assignments.
5. Select the tab System role contains to assign child system roles.
   - Assign system roles in Add assignments.
     - OR -
     Delete the system roles in Remove assignments.
6. Save the changes.

Related topics

- Assigning SAP products to organizations on page 173
- Assigning SAP products to business roles on page 174
- Assigning SAP products directly to employees on page 175
- Adding SAP products to the IT Shop on page 176
- Adding SAP groups, SAP roles, and SAP profiles in system roles on page 154

Adding SAP products to the IT Shop

Once an SAP product has been assigned to an IT Shop shelf, it can be requested by the shop customers. To ensure the SAP product is requestable, further prerequisites need to be guaranteed.

- The SAP product must be labeled with the IT Shop option.
- The SAP product must be assigned to a service item.
- The SAP product must be also labeled with Only use in IT Shop if the SAP product can only be assigned to employees using IT Shop requests. Then, the SAP product may no longer be assigned directly to hierarchical roles.

To add an SAP product to the IT Shop

1. Select SAP R/3 | Products.
2. Select the SAP product in the result list.
3. Select Add to IT Shop.
4. In **Add assignments**, add the SAP product to the IT Shop shelves.
5. Save the changes.

**To remove an SAP product from individual IT Shop shelves**

1. Select SAP R/3 | Products.
2. Select the SAP product in the result list.
3. Select **Add to IT Shop**.
4. In **Remove assignments**, remove the SAP product from the IT Shop shelves.
5. Save the changes.

**To remove an SAP product from all IT Shop shelves**

1. Select SAP R/3 | Products.
2. Select the SAP product in the result list.
3. Select **Remove from all shelves (IT Shop)**.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

The SAP product is removed from all shelves by One Identity Manager Service. All requests and assignment requests are canceled along with the SAP product as a result.

For more detailed information about providing products in the IT Shop, see the One Identity Manager IT Shop Administration Guide.

### Related topics

- Assigning SAP products directly to employees on page 175
- Assigning SAP products to organizations on page 173
- Adding SAP products in system roles on page 175
- Assigning SAP products to business roles on page 174
- Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 156

### Additional tasks for managing SAP products

After you have entered the master data, you can run the following tasks.
Overview of the SAP product

To obtain an overview of an SAP product

1. Select SAP R/3 | Products.
2. Select the SAP product in the result list.
3. Select System role overview in the task view.

Assigning SAP groups, SAP roles and SAP profiles to an SAP product

Assign the groups, roles, and profiles you want to include to the SAP product. Employees to which you assign this SAP product, will inherit these groups, roles and profiles.

**NOTE:** Groups, roles, and profiles with Only use in IT Shop can only be assigned to SAP products that also have this option set.

**NOTE:** Groups, roles, and profiles can also be added to system roles that are not SAP products.

To assign groups to an SAP product

1. Select SAP R/3 | Products.
2. Select the SAP product in the result list.
3. Select the task Assign SAP groups.
4. Assign groups in Add assignments.
   - OR -
   Remove groups from Remove assignments.
5. Save the changes.

To assign profiles to an SAP product.

1. Select SAP R/3 | Products.
2. Select the SAP product in the result list.
3. Select the task Assign SAP profiles.
4. Assign profiles in Add assignments.
   - OR -
   In Remove assignments, remove the profiles.
5. Save the changes.
To assign roles to an SAP product

1. Select SAP R/3 | Products.
2. Select the SAP product in the result list.
3. Select Assign SAP roles.
4. Assign roles in Add assignments.
   - OR -
   In Remove assignments, remove the roles.
5. Save the changes.

Related topics

- Assigning SAP products to employees on page 173

Assigning account definitions to an SAP product

Use this task to add account definitions to an SAP product. If you assign the SAP product to employees, the account definitions contained in the SAP product are inherited by the employees.

![NOTE: Account definitions roles with Only use in IT Shop set can only be assigned to SAP products that also have this option set.]

To assign account definition to an SAP product

1. Select SAP R/3 | Products.
2. Select the SAP product in the result list.
3. Select Assign account definitions.
4. Assign account definitions in Add assignments.
   - OR -
   In Remove assignments, remove the account definitions.
5. Save the changes.

Detailed information about this topic

- Setting up account definitions
Assigning subscribable reports to SAP products

Installed modules: Report Subscription Module

Use this task to add subscribable reports to an SAP product. If you assign the SAP product to employees, the subscribable reports contained in the SAP product are inherited by the employees.

**NOTE:** Subscribable reports with Only use in IT Shop set can only be assigned to SAP products that also have this option set.

**To assign subscribable reports to an SAP product**

1. Select SAP R/3 | Products.
2. Select the SAP product in the result list.
3. Select Assign subscribable reports in the task view.
4. Assign subscribable reports in Add assignments.
   - OR -
   In Remove assignments, remove the subscribable reports.
5. Save the changes.

**Detailed information about this topic**

- One Identity Manager Report Subscriptions Administration Guide

Assigning extended properties to an SAP product

Extended properties are meta objects that cannot be mapped directly in One Identity Manager, for example, operating codes, cost codes or cost accounting areas.

**To specify extended properties for an SAP product**

1. Select SAP R/3 | Products.
2. Select the SAP product in the result list.
3. Select Assign extended properties in the task view.
4. Assign extended properties in Add assignments.
   - OR -
   Remove extended properties from Remove assignments.
5. Save the changes.

Related topics
- Assigning extended properties to SAP groups, SAP roles and SAP profiles on page 166

Editing conflicting system roles

Table 77: Configuration parameters for editing mutually exclusive roles

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER\Structures\Inherite\ESetExclusion</td>
<td>Preprocessor-relevant configuration parameter for defining the effectiveness of system roles. If this parameter is set, mutually excluding system roles can be defined. The database must be recompiled after changes have been made to the parameter.</td>
</tr>
</tbody>
</table>

It is possible that employees may not own certain groups, roles and profiles at the same time. To avoid this, you can assign mutually exclusive groups, roles and profiles to different SAP products. Define these SAP products afterward as conflicting system roles. This means that conflicting system roles can be grouped together into a system role.

NOTE: Only SAP products, which are defined directly as conflicting system roles cannot be assigned to the same employee. Definitions made on parent or child SAP products do not affect the assignment.

To implement conflicting system roles
- In Designer, set the configuration parameter "QER\Structures\Inherite\ESetExclusion" and compile the database.

To define conflicting system roles
1. Select SAP R/3 | Products.
2. Select the SAP product in the result list for which you want to define conflicting system roles.
3. Select Edit conflicting system roles.
4. Double-click on the system roles in Add assignments to exclude them from the selected SAP product.
   - OR -
   In Remove assignments, double-click on the system roles that are no longer mutually exclusive.
5. Save the changes.
Providing system measurement data

User account license information can be mapped in One Identity Manager. An employee can have several user accounts which belong to different clients and systems. The employee's most significant user account is required for system measurement. This user account is determined as a chargeable user account by system measurement. One Identity Manager calculates user account ratings from the licenses assigned.

The employee's most significant user account is automatically determined from all user accounts not managed though CUA. CUA user accounts are mapped in the license information in One Identity Manager and can be edited. The most significant user account is not, however, determined automatically.

System measurement data is supplied in One Identity Manager. The actual measurement takes place in the target system.

To make system measurement data available

1. Set Enable system measurement in the SAP system.
2. Set Has user administration in the client.
3. Enter the license data
   a. Enter the license for roles and profiles. One Identity Manager finds the user account's licenses from the licenses of all roles and profiles in which the user account is a member.
      - OR -
   b. Enter the active license directly in the user account.

One Identity Manager calculates the most significant user account license from the licenses entered.

4. Publish the measurement data.

The calculated licenses are transferred to the active licenses. Active licenses are published in the target system. System measurement can be carried out there.

Detailed information about this topic

- SAP systems on page 102
- General master data for an SAP client on page 103
Mapping the measurement data

Measurement data is displayed on the master data form for user accounts which are not CUA.

To display measurement data

1. Select SAP R/3 | User accounts.
2. Select the user account in the result list.
3. Change to Inventory data.

This opens the master data form with synchronized and calculated data for system measurement.

The following license information is displayed on the form.

Table 78: User account measurement data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active License</td>
<td>User account's license. The active license is loaded into the One Identity Manager database by synchronization or found from the calculated, employee-related license.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The active license can also be edited directly and changed. Changes to the active license are published immediately in the target system. The licenses stored with the roles and profiles are not effective in this case.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If licenses are stored with roles or profiles in which the user account is a member and Publishing calculated licenses is running, the active license stored directly with the user account is overwritten by the calculated license.</td>
</tr>
<tr>
<td>Special version ID</td>
<td>License extension for the installed special version. Select the special version ID from the menu. This is only enabled if special versions are permitted for the active license.</td>
</tr>
<tr>
<td>Country surcharge</td>
<td>Additional license fee. This is only enabled if country surcharges are permitted for the active license.</td>
</tr>
<tr>
<td>Substitute</td>
<td>Link to the user account which takes over as deputy for a specified time period. This field is only active if &quot;04 (substitute)&quot; or &quot;11 (Multi-client/system)&quot; is entered. The substitute user account obtains roles and profiles of</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>the displayed user account</td>
<td>for a specified time period.</td>
</tr>
<tr>
<td>Substituted from</td>
<td>Time period in which another user account assumes responsibility. This input field is enabled if the active license is set to &quot;04 (substitute)&quot;.</td>
</tr>
<tr>
<td>Substituted until</td>
<td></td>
</tr>
<tr>
<td>Calculated license (client)</td>
<td>License determined from user account assigned roles and profiles within the client.</td>
</tr>
<tr>
<td>Calculated license (employee)</td>
<td>License of most significant employee user account. The client related calculated license is entered for the most significant user account. For all the other employee's user accounts, the employee related calculated license &quot;11 (Multi-client/system user)&quot; is entered. This also contains a reference to the calculated most significant user account (Calculated ref. name).</td>
</tr>
<tr>
<td>Calculated ref. name</td>
<td>Link to the calculated most significant user account if &quot;11 (Multi-client/system user)&quot; is entered.</td>
</tr>
</tbody>
</table>

Measurement data is displayed for each user account assignment to the target system and to child systems if the user accounts are managed over CUA,

**To display measurement data for a centrally administered user account**

1. Select the **SAP R/3 | User accounts** category.
2. Select the user account in the result list.
3. Select **SAP Assign licenses in client systems**.
4. Select an assignment in the table.

The following license information is displayed on the form.

**Table 79: Measurement Data for a Centrally administrated User Account**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipient client</td>
<td>Client containing the user account which is assigned a license. You can select the central system or a assigned child system.</td>
</tr>
<tr>
<td>License</td>
<td>User account license in the selected client.</td>
</tr>
<tr>
<td>License extension</td>
<td>License extension for the installed special version. Select the special version ID from the menu.</td>
</tr>
<tr>
<td>Country surcharge</td>
<td>Additional license fee.</td>
</tr>
<tr>
<td>Chargeable</td>
<td>SAP system containing the client to be charged. This field is only shown if...</td>
</tr>
</tbody>
</table>
## Related topics

- [Entering licenses for SAP user accounts](#) on page 185
- [Determining licenses using SAP roles and SAP profiles](#) on page 186
- [Determining the rating of an SAP user account](#) on page 187
- [Transferring calculated licenses](#) on page 189
- [Special versions](#) on page 81
- [Licenses](#) on page 80

## Entering licenses for SAP user accounts

In order to maintain system measurement data directly in user accounts, enter the active license in the user accounts. This might be necessary, for example, for storing substitute licenses.

### To enter a user account active license

1. Select **SAP R/3 | User accounts**.
2. Select the user account in the result list.
3. Select **Measurement data**.
4. Select **Active license**.
5. Enter any other data required, if necessary.
6. Save the changes.

The active license is published in the target system.

NOTE: If licenses are stored with roles or profiles in which the user account is a member and **Publishing calculated licenses** is running, the active license stored directly with the user account is overwritten by the calculated license.
To enter the centrally administrated user account's license

1. Select the SAP R/3 | User accounts category.
2. Select the user account in the result list.
3. Select SAP Assign licenses in client systems.
4. Click Add.
   This inserts a new row in the table.
5. Mark this row. Enter the measurement data.
6. Save the changes.

Detailed information about this topic

- Mapping the measurement data on page 183
- Determining licenses using SAP roles and SAP profiles on page 186

Determining licenses using SAP roles and SAP profiles

The most significant license can be determined from role and profile licenses that are not managed through CUA. You must make the initial assignment of licenses manually after synchronizing roles and profiles. One Identity Manager determines the user account's highest rated license through user account memberships in roles and profiles. The employee's most significant user account is found across clients and system. The most significant license is added to the user account as the active license and published in the target system.

To assign roles and profiles

1. Select SAP R/3 | Roles.
   - OR -
   Select SAP R/3 | Profiles.
2. Select the role or profile in the result list.
3. Assign a license in License.
4. Save the changes.

Related topics

- Licenses on page 80
- General master data for SAP profiles on page 146
- General master data for SAP roles on page 145
Determining the rating of an SAP user account

NOTE: In this section, roles and profiles are grouped under the term "SAP system entitlements" to make it easier to understand.

A rating for a user account is determined in One Identity Manager by rating profiles and roles in which the user account is a member. Licenses have to be entered for the profiles and roles as a prerequisite. You have to make this assignment once manually after the objects have been synchronized. When the most significant user account is determined, the license names and any manually issued license value are taken into account.

A recalculation task for the DBQueue Processor is generated to determine license rating. The recalculation task is generated when:

- **System measurement enabled** for the SAP system is disabled/enabled.
- **Has user account management** for the SAP client is disabled/enabled.
- User account assignments to roles or profiles are changed
- Role assignment validity periods are changed
- License's rating changes
- License assignments to roles or profiles are changed
- Employee assignment to user accounts
- The user account substitute is changed

The most highly rated user account is determined in One Identity Manager in a two-step process.

1. **Determining the significance of a user account within a client (client related)**
   
   Memberships in system entitlements within a client are calculated for an SAP user account. Through this, the SAP system entitlement with the highest rating is found. The license for the most significant SAP system entitlement is added to the user account as **Calculated license (client)**. The most significant SAP system entitlement meets the following criteria:
   
   a. The assigned license has the lowest license rating (in alphanumeric sort order).
   
   b. If several SAP system entitlements with the same license rating are assigned or no license rating has been given, the valid license is that with the highest rating.

2. **Determining the most highly rated user account (employee related)**

   a. The most significant user account is determined from all the employee’s user account in all clients and all systems. The criteria from 1a) and 1b) apply for these user accounts. The license for the most highly rated user account is added to the user account as **Calculated license (employee)**. A reference to the user account calculated with the most significance is entered for all of the employee’s other user accounts in **Calculated ref. name**. These user account contain the license "11 (Multi-client/system) or "04 (substitute)".
Table 80: Employee-related license

<table>
<thead>
<tr>
<th>User accounts</th>
<th>Calculated license (employee)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most significant user account</td>
<td>Calculated license (client)</td>
</tr>
<tr>
<td>Remaining user accounts in clients of the same system as the most significant user account</td>
<td>04 (Deputy manager or supervisor)</td>
</tr>
<tr>
<td>Remaining user accounts in other systems besides the most significant user account</td>
<td>11 (Multi-client/system)</td>
</tr>
</tbody>
</table>

b. If a user account is not assigned an employee, the rating calculated under 1) is seen as the most significant and the license entry is added to the user account as **Calculated license (employee)**.

**Figure 5: Determining an SAP User Account Rating**

**Related topics**

- **Licenses** on page 80
Transferring calculated licenses

In order to execute system measurement in the SAP R/3 environment, you need to transfer employee related calculated licenses to the active license. This transfer is done separately for each client in the system.

**NOTE:** If **Publishing calculated licenses** is run, the active license stored directly with the user account is overwritten by the calculated license!

Exception: "04 (substitute)" is entered as active license and the substitute time period is currently valid or is in the future.

**NOTE:** **Publishing calculated licenses** is only for clients with CUA status "No CUA system" or empty CUA status.

To transfer calculated licenses to active licenses

1. Select **SAP R/3 | Clients**.
2. Select the client whose licenses are to be transferred.
3. Select **Publish calculated licenses**.
   - A security prompt appears.
4. Confirm the security prompt with **Yes**.

Once the calculated licenses are transferred to active licenses, the active licenses are published in the target system.

One Identity Manager transfers the calculated employee related license for all this client's user accounts to the active license. You can edit this data later, if required. Once the licenses are published in the SAP R/3 system and system measurement has been carried out, you can synchronize the current measurement data with the One Identity Manager database.

Special characteristics of user accounts with a deputy license

If the active license "04 (substitute)" is entered in the user account and the substitution period is current valid, the active license is not replaced by the calculated employee-related license. The same applies if the substitution period is in the future (**Substituted from** later than "today").

If the substitution period has expired, the calculated employee-related license is transferred to the active license by the task **Publishing calculated licenses**.

Information about the substitute and the substitution period is deleted from the user account.

**NOTE:** In order to publish an active license "04 (substitute)" in the target system, the price list and all usable user types must be enabled in the program part system measurement in the SAP R/3 environment.
Related topics

- Mapping the measurement data on page 183
Reports about SAP systems

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. The following reports are available for SAP systems.

**NOTE:** Other sections may be available depending on the which modules are installed.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of all assignments (system)</td>
<td>This report finds all roles containing employees with at least one user account in the selected system.</td>
</tr>
<tr>
<td>Overview of all assignments (client)</td>
<td>This report identifies all roles containing employees with at least one user account in the selected client.</td>
</tr>
<tr>
<td>Overview of all assignments (group, role, profile)</td>
<td>This report find all roles containing employees with the selected group, role or profile.</td>
</tr>
<tr>
<td>Show orphaned user accounts</td>
<td>This report shows all user accounts in the client that are not assigned to an employee. The report contains assigned system entitlements and risk assessment.</td>
</tr>
<tr>
<td>Show employees with multiple user accounts</td>
<td>This report shows all employees with more than one user account in the client. The report contains a risk assessment.</td>
</tr>
<tr>
<td>Show system entitlement drifts</td>
<td>This report shows all the client's system entitlements that are the result of manual operations in the target system rather than using the One Identity Manager provisioning engine.</td>
</tr>
<tr>
<td>Show unused user accounts</td>
<td>This report shows all the client's user accounts that have not been used in the last few months.</td>
</tr>
<tr>
<td>Show user accounts with an above average number of system entitlements</td>
<td>This report contains all the client's user accounts with an above average number of system entitlements.</td>
</tr>
</tbody>
</table>
### Overview of all assignments

The **Overview of all assignments** report is displayed for some objects, such as authorizations, compliance rules, or roles. The report finds all the roles, for example, departments, cost centers, locations, business roles and IT Shop structures in which there are employee who own the selected base object. In this case, direct as well as indirect base object assignments are included.

#### Examples

- If the report is created for a resource, all roles are determined in which there are employees with this resource.
- If the report is created for a group or another system entitlement, all roles are determined in which there are employees with this group or system entitlement.
- If the report is created for a compliance rule, all roles are determined in which there are employees who violate this compliance rule.
- If the report is created for a department, all roles are determined in which employees of the selected department are also members.
- If the report is created for a business role, all roles are determined in which employees of the selected business role are also members.

#### To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the report **Overview of all assignments**.
- Click the **Used by** button in the report toolbar to select the role class for which you want to determine whether roles exist that contain employees with the selected base object.

  All the roles of the selected role class are shown. The color coding of elements identifies the role in which there are employees with the selected base object. The meaning of the report control elements is explained in a separate legend. To access the legend, click the ![icon](image) icon in the report’s toolbar.

- Double-click a control to show all child roles belonging to the selected role.
- By clicking the ⬇️ button in a role's control, you display all employees in the role with the base object.
- Use the small arrow next to ⬇️ to start a wizard that allows you to bookmark this list of employee for tracking. This creates a new business role to which the employees are assigned.

Figure 6: Toolbar of the Overview of all assignments report.

Table 82: Meaning of Icons in the Report Toolbar

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>📘</td>
<td>Show the legend with the meaning of the report control elements</td>
</tr>
<tr>
<td>📁</td>
<td>Saves the current report view as a graphic.</td>
</tr>
<tr>
<td>🤧</td>
<td>Selects the role class used to generate the report.</td>
</tr>
<tr>
<td>⬇️</td>
<td>Displays all roles or only the affected roles.</td>
</tr>
</tbody>
</table>
Appendix: Configuration parameters for managing an SAP R/3 environment

The following configuration parameters are additionally available in One Identity Manager after the module has been installed.

**Table 83: Configuration parameters**

<table>
<thead>
<tr>
<th>Configuration parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetSystem\SAPR3</td>
<td>SAP is supported. The parameter is a precompiler dependent configuration parameter. Changes to the parameter require recompiling the database.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts</td>
<td>Default values should be used for SAP user accounts.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Datfm</td>
<td>Specifies the default date format for SAP user accounts.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Dcpfm</td>
<td>Specifies the default decimal point format for SAP user accounts.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\ExtID_Type</td>
<td>Specifies the default type for external identification of SAP user accounts.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Fax_Group</td>
<td>Specifies the default fax group for SAP user accounts.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Guiflag</td>
<td>Specifies whether secure communication is permitted for SAP user accounts.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\InitialRandomPassword</td>
<td>This configuration parameter specifies whether a random...</td>
</tr>
<tr>
<td>Configuration parameters</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\InitialRandomPassword\SendTo</td>
<td>generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName</td>
<td>This configuration parameter specifies to which employee the email with the random generated password should be sent (manager cost center-department/location/business role, employee’s manager or XUserInserted). If no recipient can be found, the password is sent to the address stored in the “TargetSystem\SAPR3\DefaultAddress” configuration parameter.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword</td>
<td>This configuration parameter contains the name of the mail template sent to provide users with the login data for their user accounts. The Employee - new user account created mail template is used.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Language_p</td>
<td>Specifies default language key for SAP users.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Langup_iso</td>
<td>Specifies default language (ISO 639).</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\MailTemplateDefaultValues</td>
<td>This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account. The Employee -</td>
</tr>
<tr>
<td>Configuration parameters</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Spda</td>
<td>Specifies default setting for printer parameter 3 (delete after print).</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Spdb</td>
<td>Specifies default setting for printer parameter 3 (print immediately).</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Spig</td>
<td>Specifies the default printer (print parameter 1).</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\TargetSystemID</td>
<td>Specifies default target system identification for mapping external users.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Time_zone</td>
<td>Specifies the default time zone value for the SAP user account’s address.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Tzone</td>
<td>Specifies the default value for the time zone.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\Accounts\Ustyp</td>
<td>Specifies the default user type for SAP user accounts.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\DefaultAddress</td>
<td>Default email address (recipient) for messages about actions in the target system.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\KeepRedundantProfiles</td>
<td>This configuration parameter regulates behavior for handling single role and profile assignments to users.</td>
</tr>
<tr>
<td></td>
<td>If the parameter is set, the user's single roles or profiles, which are already part of the user's collective roles, are retained.</td>
</tr>
<tr>
<td></td>
<td>If the parameter is not set, the user's single roles or profiles, which are already part of the user's collective roles, are removed (default).</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\MaxFullsyncDuration</td>
<td>Specifies the maximum runtime for synchronization.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\PersonAutoDefault</td>
<td>This configuration parameter</td>
</tr>
<tr>
<td>Configuration parameters</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\PersonAutoDisabledAccounts</td>
<td>This configuration parameter specifies whether employees are automatically assigned to disable user accounts. User accounts do not obtain an account definition.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\PersonAutoFullSync</td>
<td>This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\ValidDateHandling</td>
<td>Configuration parameter for handling the validity period in SAP user account assignments to SAP roles.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\ValidDateHandling\DoNotUsePWODate</td>
<td>This configuration parameter specifies whether the validity dates from request procedure are copied from SAP user account assignments to SAP roles. If the configuration parameter is set, the dates, &quot;Valid from&quot; and &quot;Valid to&quot; from the request procedure, are not copied from SAP user account assignments to SAP roles.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\ValidDateHandling\ReuseInheritedDate</td>
<td>This configuration parameter specifies whether the validity date's format of inherited SAP user account assignments to SAP roles remains intact. The configuration parameter is only relevant in systems that were migrated from a pre 7.0 version. If the configuration parameter is set, the format of the dates &quot;Valid from&quot; and &quot;Valid to&quot; stays the same if SAP user account assignments to roles are inherited.</td>
</tr>
<tr>
<td>Configuration parameters</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\ValidDateHandling\ReuseInheritedDate\UseTodayForInheritedValidFrom</td>
<td>This configuration parameter specifies whether the &quot;Valid from&quot; date in inherited SAP user accounts assignments to SAP roles is set to &lt;Today&gt; or to &quot;1900-01-01&quot;.</td>
</tr>
<tr>
<td>TargetSystem\SAPR3\VerifyUpdates</td>
<td>This configuration parameter specifies whether modified properties are checked by updating. If this parameter is set, the objects in the target system are verified after every update.</td>
</tr>
</tbody>
</table>
Appendix: Default project templates for synchronizing an SAP R/3 environment

A default project template ensures that all required information is added in One Identity Manager. This includes mappings, workflows and the synchronization base object. If you do not use a default project template you must declare the synchronization base object in One Identity Manager yourself.

Use a default project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor.

Detailed information about this topic

- Project template for client without CUA on page 199
- Project template for the CUA central system on page 201
- Project template for CUA subsystems on page 202

Project template for client without CUA

Use "SAP® R/3® synchronization (base administration)" to synchronize clients that are not connected to a central user administration. The template uses mappings for the following schema types.

Table 84: Mapping SAP R/3 schema types to tables in the One Identity Manager schema.

<table>
<thead>
<tr>
<th>Schema Type in the Target System</th>
<th>Table in the One Identity Manager Schema</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company</td>
<td>SAPCompany</td>
</tr>
<tr>
<td>Schema Type in the Target System</td>
<td>Table in the One Identity Manager Schema</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>GROUP</td>
<td>SAPGrp</td>
</tr>
<tr>
<td>LICENSETYPE</td>
<td>SAPLicence</td>
</tr>
<tr>
<td>LicenceExtension</td>
<td>SAPLicenceExtension</td>
</tr>
<tr>
<td>LoginLanguage</td>
<td>SAPLoginLanguages</td>
</tr>
<tr>
<td>CLIENT</td>
<td>SAPMandant</td>
</tr>
<tr>
<td>Parameter</td>
<td>SAPParameter</td>
</tr>
<tr>
<td>Printer</td>
<td>SAPPrinter</td>
</tr>
<tr>
<td>PROFILE</td>
<td>SAPProfile</td>
</tr>
<tr>
<td>ProfileInProfile</td>
<td>SAPProfileInSAPProfile</td>
</tr>
<tr>
<td>ProfileInRole</td>
<td>SAPProfileInSAPRole</td>
</tr>
<tr>
<td>PROFITCENTER</td>
<td>SAPProfitCenter</td>
</tr>
<tr>
<td>ROLE</td>
<td>SAPRole</td>
</tr>
<tr>
<td>RoleInRole</td>
<td>SAPRoleInSAPRole</td>
</tr>
<tr>
<td>STARTMENUE</td>
<td>SAPStartMenu</td>
</tr>
<tr>
<td>SAPTSAD3T</td>
<td>SAPTitle</td>
</tr>
<tr>
<td>USER</td>
<td>SAPUser</td>
</tr>
<tr>
<td>UserComFax</td>
<td>SAPComFax</td>
</tr>
<tr>
<td>UserComPhone</td>
<td>SAPComPhone</td>
</tr>
<tr>
<td>UserComSMTP</td>
<td>SAPComSMTP</td>
</tr>
<tr>
<td>SAPCOMMTYPE</td>
<td>SAPCommType</td>
</tr>
<tr>
<td>UserExtId</td>
<td>SAPUserExtId</td>
</tr>
<tr>
<td>UserHasParameter</td>
<td>SAPUserHasParameter</td>
</tr>
<tr>
<td>UserInGroup</td>
<td>SAPUserInSAPGrp</td>
</tr>
<tr>
<td>UserInProfile</td>
<td>SAPUserInSAPProfile</td>
</tr>
<tr>
<td>UserInRole</td>
<td>SAPUserInSAPRole</td>
</tr>
</tbody>
</table>
Project template for the CUA central system

Use "SAP® R/3® synchronization (base administration)" to synchronize a central user administration central system. The template uses mappings for the following schema types.

Table 85: Mapping SAP R/3 schema types to tables in the One Identity Manager schema.

<table>
<thead>
<tr>
<th>Schema Type in the Target System</th>
<th>Table in the One Identity Manager Schema</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALE</td>
<td>SAPMandant</td>
</tr>
<tr>
<td>CLIENT</td>
<td>SAPMandant</td>
</tr>
<tr>
<td>Company</td>
<td>SAPCompany</td>
</tr>
<tr>
<td>GROUP</td>
<td>SAPGrp</td>
</tr>
<tr>
<td>LICENSETYPE</td>
<td>SAPLicence</td>
</tr>
<tr>
<td>LicenceExtension</td>
<td>SAPLicenceExtension</td>
</tr>
<tr>
<td>LoginLanguage</td>
<td>SAPLoginLanguages</td>
</tr>
<tr>
<td>Parameter</td>
<td>SAPParameter</td>
</tr>
<tr>
<td>Printer</td>
<td>SAPPrinter</td>
</tr>
<tr>
<td>CUAProfile</td>
<td>SAPProfile</td>
</tr>
<tr>
<td>ProfileInProfile</td>
<td>SAPProfileInSAPProfile</td>
</tr>
<tr>
<td>ProfileInRole</td>
<td>SAPProfileInSAPRole</td>
</tr>
<tr>
<td>PROFITCENTER</td>
<td>SAPProfitCenter</td>
</tr>
<tr>
<td>CUARole</td>
<td>SAPRole</td>
</tr>
<tr>
<td>RoleInRole</td>
<td>SAPRoleInSAPRole</td>
</tr>
<tr>
<td>STARTMENUE</td>
<td>SAPStartMenu</td>
</tr>
<tr>
<td>SAPTSAD3T</td>
<td>SAPTitle</td>
</tr>
<tr>
<td>USER</td>
<td>SAPUser</td>
</tr>
<tr>
<td>UserComFax</td>
<td>SAPComFax</td>
</tr>
<tr>
<td>UserComPhone</td>
<td>SAPComPhone</td>
</tr>
<tr>
<td>UserComSMTP</td>
<td>SAPComSMTP</td>
</tr>
<tr>
<td>Schema Type in the Target System</td>
<td>Table in the One Identity Manager Schema</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>UserExtId</td>
<td>SAPUserExtId</td>
</tr>
<tr>
<td>UserHasLicense</td>
<td>SAPUserHasLicence</td>
</tr>
<tr>
<td>UserHasParameter</td>
<td>SAPUserHasParameter</td>
</tr>
<tr>
<td>UserInGroup</td>
<td>SAPUserInSAPGrp</td>
</tr>
<tr>
<td>UserInMandant</td>
<td>SAPUserInSAPMandant</td>
</tr>
<tr>
<td>UserInCUAPerfile</td>
<td>SAPUserInSAPProfile</td>
</tr>
<tr>
<td>UserInCUARole</td>
<td>SAPUserInSAPRole</td>
</tr>
</tbody>
</table>

**Project template for CUA subsystems**

Use the "SAP® R/3® (CUA subsystem)" project template to synchronize central user administration child systems that are not in the same SAP system. The template uses mappings for the following schema types.

**Table 86: Mapping SAP R/3 schema types to tables in the One Identity Manager schema.**

<table>
<thead>
<tr>
<th>Schema Type in the Target System</th>
<th>Table in the One Identity Manager Schema</th>
</tr>
</thead>
<tbody>
<tr>
<td>LICENSETYPE</td>
<td>SAPLicence</td>
</tr>
<tr>
<td>LicenceExtension</td>
<td>SAPLicenceExtension</td>
</tr>
<tr>
<td>LoginLanguage</td>
<td>SAPLoginLanguages</td>
</tr>
<tr>
<td>CLIENT</td>
<td>SAPMandant</td>
</tr>
</tbody>
</table>
Appendix: Referenced SAP R/3 tables and BAPI calls

The following overview provides information about all the tables in an SAP R/3 system referenced during synchronization and the BAPI calls that are executed.

Table 87: Referenced tables and BAPIs

<table>
<thead>
<tr>
<th>Tables</th>
<th>BAPI Calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADR2</td>
<td>BAPI_USER_CREATE1</td>
</tr>
<tr>
<td>ADR3</td>
<td>BAPI_USER_GET_DETAIL</td>
</tr>
<tr>
<td>ADR6</td>
<td>BAPI_USER_CHANGE</td>
</tr>
<tr>
<td>AGR_1016</td>
<td>BAPI_USER_DELETE</td>
</tr>
<tr>
<td>AGR_AGRS</td>
<td>BAPI_USER_LOCK</td>
</tr>
<tr>
<td>AGR_DEFINE</td>
<td>BAPI_USER_UNLOCK</td>
</tr>
<tr>
<td>AGR_USERS</td>
<td>BAPI_USER_ACTGROUPS_ASSIGN</td>
</tr>
<tr>
<td>ANLA</td>
<td>BAPI_USER_ACTGROUPS_DELETE</td>
</tr>
<tr>
<td>ANLZ</td>
<td>BAPI_USER_PROFILES_ASSIGN</td>
</tr>
<tr>
<td>CSKS</td>
<td>BAPI_USER_PROFILES_DELETE</td>
</tr>
<tr>
<td>CSKT</td>
<td>BAPI_USER_LOCACTGROUPS_READ</td>
</tr>
<tr>
<td>DD02L</td>
<td>BAPI_USER_LOCACTGROUPS_DELETE</td>
</tr>
<tr>
<td>DD03L</td>
<td>BAPI_USER_LOCPROFILES_READ</td>
</tr>
<tr>
<td>DD04L</td>
<td>BAPI_USER_LOCPROFILES_DELETE</td>
</tr>
<tr>
<td>DD07L</td>
<td>BAPI_USER_SYSTEM_ASSIGN</td>
</tr>
<tr>
<td>RSECUSERAUTH</td>
<td>SUSR_USER_CHANGE_PASSWORD_RFC</td>
</tr>
<tr>
<td>RSECTX</td>
<td>BAPI_USER_LOCPROFILES_ASSIGN</td>
</tr>
<tr>
<td>SEC_POLICY_CUST</td>
<td>BAPI_USER_LOCACTGROUPS_ASSIGN</td>
</tr>
<tr>
<td>SEC_POLICY_RT</td>
<td>RFC_READ_TABLE</td>
</tr>
</tbody>
</table>
## Tables

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>T000</td>
<td></td>
</tr>
<tr>
<td>T001</td>
<td></td>
</tr>
<tr>
<td>T002</td>
<td></td>
</tr>
<tr>
<td>T591S</td>
<td></td>
</tr>
<tr>
<td>T500P</td>
<td></td>
</tr>
<tr>
<td>T548T</td>
<td></td>
</tr>
<tr>
<td>TMENU01</td>
<td></td>
</tr>
<tr>
<td>TMENU01R</td>
<td></td>
</tr>
<tr>
<td>TPARA</td>
<td></td>
</tr>
<tr>
<td>TSAD3</td>
<td></td>
</tr>
<tr>
<td>TSAD3T</td>
<td></td>
</tr>
<tr>
<td>TSAC</td>
<td></td>
</tr>
<tr>
<td>TSADC</td>
<td></td>
</tr>
<tr>
<td>TSP03</td>
<td></td>
</tr>
<tr>
<td>TTREE</td>
<td></td>
</tr>
<tr>
<td>TUTYPA</td>
<td></td>
</tr>
<tr>
<td>TUTYPPL</td>
<td></td>
</tr>
<tr>
<td>TUZUS</td>
<td></td>
</tr>
<tr>
<td>USGRP_USER</td>
<td></td>
</tr>
<tr>
<td>USL04</td>
<td></td>
</tr>
<tr>
<td>USLA04</td>
<td></td>
</tr>
<tr>
<td>USR01</td>
<td></td>
</tr>
<tr>
<td>USR02</td>
<td></td>
</tr>
<tr>
<td>USR05</td>
<td></td>
</tr>
<tr>
<td>USR06</td>
<td></td>
</tr>
<tr>
<td>USR06SYS</td>
<td></td>
</tr>
<tr>
<td>USR12</td>
<td></td>
</tr>
<tr>
<td>USR21</td>
<td></td>
</tr>
<tr>
<td>USREFUS</td>
<td></td>
</tr>
<tr>
<td>USREXTID</td>
<td></td>
</tr>
<tr>
<td>UST04</td>
<td></td>
</tr>
<tr>
<td>UST10C</td>
<td></td>
</tr>
<tr>
<td>USZBVLNDS</td>
<td></td>
</tr>
<tr>
<td>Tables</td>
<td>BAPI Calls</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>USZBVLNDCRC</td>
<td></td>
</tr>
<tr>
<td>USZBV SYS</td>
<td></td>
</tr>
<tr>
<td>USRSYSACCTT</td>
<td></td>
</tr>
<tr>
<td>USRSYS PRF</td>
<td></td>
</tr>
<tr>
<td>USRSTAMP</td>
<td></td>
</tr>
<tr>
<td>V_USCOMPA</td>
<td></td>
</tr>
</tbody>
</table>
Appendix: Example of a schema extension file

<?xml version="1.0" encoding="utf-8" ?>
<SAP>

   <Functions>
      <Function Definition = "USER GET" FunctionName="BAPI_USER_GET_DETAIL"
          OutStructure = "" Key ="USERNAME" X500 ="CN">
          <Mapping>
             <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
          </Mapping>
      </Function>

      <Function Definition = "USER SET" FunctionName="BAPI_USER_CHANGE"
          OutStructure ="" Key ="USERNAME" X500 ="CN">
          <Mapping>
             <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
          </Mapping>
      </Function>

      <Function Definition = "USER DEL" FunctionName="BAPI_USER_DELETE"
          OutStructure ="" Key ="USERNAME" X500 ="CN">
          <Mapping>
             <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
          </Mapping>
      </Function>

      <Function Definition = "USER PROFILE SET" FunctionName="BAPI_USER_PROFILES_ASSIGN"
          OutStructure ="" Key ="USERNAME" X500 ="CN">
          <Mapping>
             <Data ParameterName = "USERNAME" PropertyName = "BNAME" />
          </Mapping>
      </Function>
   </Functions>

</SAP>
<Data ParameterName = "BAPIPROF~BAPIPROF" PropertyName = "$Value$" />
</Mapping>
</Function>

<Function Definition = "BWProfileAdd" FunctionName="/VIAENET/SAPHR_RSECUSERAUT_ADD" OutStructure ="" Key ="ZUSRNAME,ZHIER" X500 ="CN,OU">
  <Mapping>
    <Data ParameterName = "ZUSRNAME" PropertyName = "UNAME" />
    <Data ParameterName = "ZHIER" PropertyName = "AUTH" />
  </Mapping>
</Function>

<Function Definition = "BWProfileDel" FunctionName="/VIAENET/SAPHR_RSECUSERAUT_DEL" OutStructure ="" Key ="ZUSRNAME,ZHIER" X500 ="CN,OU">
  <Mapping>
    <Data ParameterName = "ZUSRNAME" PropertyName = "UNAME" />
    <Data ParameterName = "ZHIER" PropertyName = "AUTH" />
  </Mapping>
</Function>

<Function Definition = "BWProfileDelFkt" FunctionName="/VIAENET/SAPHR_RSECUSERAUT_DEL" OutStructure ="" Key ="ZUSRNAME,ZHIER" X500 ="CN,OU">
  <Mapping>
    <Data ParameterName = "ZUSRNAME" PropertyName = "BNAME" />
    <Data ParameterName = "ZHIER" PropertyName = "$VALUE$" />
  </Mapping>
</Function>

<Function Definition = "BWProfileAddFkt" FunctionName="/VIAENET/SAPHR_RSECUSERAUT_ADD" OutStructure ="" Key ="ZUSRNAME,ZHIER" X500 ="CN,OU">
  <Mapping>
    <Data ParameterName = "ZUSRNAME" PropertyName = "BNAME" />
    <Data ParameterName = "ZHIER" PropertyName = "$VALUE$" />
  </Mapping>
</Function>
</Functions>

<Tables>
  <TABLE Definition = "TUZUS-Table" TableName="TUZUS" Key="SONDERVERS" X500="CN" SQL="LANGU = sy-langu" Load="SONDERVERS,TEXTSVERS" />
</Tables>
<TABLE Definition = "USR05-Table" TableName="USR05" Key="BNAME,PARID" X500="CN,OU" SQL="MANDT = '$MANDT$'" Load="BNAME,PARID,PARVA">
  <Mapping>
    <Data ParameterName = "$BNAME$" PropertyName = "BNAME" />
    <Data ParameterName = "$PARID$" PropertyName = "PARID" />
  </Mapping>
</TABLE>

<TABLE Definition = "USR04-Table" TableName="USR04" Key="BNAME,MANDT" X500="CN,OU" SQL="MANDT = sy-mandt" Load="" />
<TABLE Definition = "RSECUSERAUTH-Table" TableName="RSECUSERAUTH" Key="UNAME,AUTH" X500="CN,OU" SQL="" Load="" />
<TABLE Definition = "RSECUSERAUTH-SingleUser" TableName="RSECUSERAUTH" Key="AUTH" X500="CN" SQL="UNAME = '$BNAME$'" Load="" >
  <Mapping>
    <Data ParameterName = "$BNAME$" PropertyName = "BNAME" />
  </Mapping>
</TABLE>
</Tables>

<SAPExtendedSchematypes>
  <SAPExtendedSchematype Bem = "M:N, add/del - function" Name = "BWUserInBWP" DisplayPattern="%UNAME% - %AUTH%" ListObjectsDefinition = "RSECUSERAUTH-Table" ReadObjectDefinition = "RSECUSERAUTH-Table" InsertObjectDefinition = "BWProfileAdd" DeleteObjectDefinition = "BWProfileDel" />
  <SAPExtendedSchematype Bem = "simple read only table" Name = "LicenceExtension" DisplayPattern="%SONDERVERS%" ListObjectsDefinition = "TUZUS-Table" ReadObjectDefinition = "TUZUS-Table" InsertObjectDefinition = "" WriteObjectDefinition = "" DeleteObjectDefinition = "" ParentType = "SAPSYSTEM" />
  <SAPExtendedSchematype Bem = "Test" Name = "USERFunctionTable" DisplayPattern="%BNAME% (%MANDT%)" ListObjectsDefinition = "USR05-Table" ReadObjectDefinition = "USER GET" WriteObjectDefinition = "USER SET" DeleteObjectDefinition = "USER DEL" >
    <Properties>
      <Property Name = "SAPBWP" Description="all the user's BW profiles" ListFunction="RSECUSERAUTH-SingleUser" AddFunction="BWProfileAddFkt" DelFunction="BWProfileDelFkt" ReplaceFunction="" IsMultivalued = "true" />
      <Property Name = "USERPROFILE" Description="all the user's profiles" ListFunction="USR04-Table" AddFunction="" />
DelFunction="" ReplaceFunction="USER PROFILE SET" IsMultivalued = "true" />
</Properties>
</SAPExtendedSchematype>
</SAPExtendedSchematypes>
</SAP>
About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product
A
account definition 112
  add to IT Shop 72
  assign automatically 59
  assign to business roles 70
  assign to employee 70-71, 73
  assign to roles 69
  create 59
  delete 74
  for IT Shop 59
  inheritance 59, 63, 68
account definitions
  assign to system roles 71
ALE model name 33
application role 11
application server 8
architecture 8

B
BAPI transport 16-17
  uninstall 17
business role
  assign to groups 150
  assign to products 174
  assign to profile 150
  assign to roles 150
cost center
  assign to group 148
  assign to product 173
  assign to profile 148
  assign to role 148
  SAP R/3 78
country surcharge 80, 183
CUA 112
central user administration 112
  user account 129
child system
  access permissions 112
  no synchronization 33
client 103
  category 164
  child system 103
  employee assignment 135
  login data 103
  target system manager 103
collective role
  synchronize 50
communications type 80
company address 79
collection parameter 21
connector schema
  extend 39
cost center
  assign to group 148
  assign to product 173
  assign to profile 148
  assign to role 148
  SAP R/3 78
country surcharge 80, 183
CUA 112
database server 8
department
assign to group 148
assign to product 173
assign to profile 148
assign to role 148
deputy
license data 183
direction of synchronization
direction target system 21
in the Manager 21

E
e-mail address 122
e-mail notification 93
employee assignment
manual 136
removing 136
search criteria 135
exclusion definition 161
external identifier
type 77

F
fax 121

G
group
assign business roles 150
assign cost center 148
assign department 148
assign extended property 166
assign location 148
assign shelf 156
assign system role 154
assign user account 152
category 143, 164
effective 161
exclude 161
inheritance 63
IT Shop 143
manage 142
overview 161
risk index 143

I
inheritance
category 164
IT operating data
change 67
create mapping rule 64
IT Shop shelf
assign account definition 72

J
Job server
properties 95

L
license 80
active 183
country surcharge 80
rating 80
special version 80
license extension 81
location
assign to group 148
assign to product 173
assign to profile 148
assign to role 148
deny list 90
login language 79
display name 85
logon information 93
ingit message 85
failed logins 86
generate password 91
generating script 88-89
initial password 86
generate password 81
name properties 86
password age 86
password cycle 86
password length 86
password strength 86
predefined 82
printers 78
product 170
object
assign business role 174
assign cost center 173
assign department 173
assign employee 175
assign extended properties 180
assign group 178
assign location 173
assign profile 178
assign role 178
assign system role 175
assign system role 175
conflicting system role 181
disable 171
IT Shop 171
manager 171
ownership 178
overview 178
remove from IT Shop 176
risk index 171
share date 171

assign business role 174
assign cost center 173
assign department 173
assign employee 175
assign extended properties 180
assign group 178
assign location 173
assign profile 178
assign role 178
assign system role 175
conflicting system role 181
disable 171
IT Shop 171
manager 171
ownership 178
overview 178
remove from IT Shop 176
risk index 171
share date 171
profile
    assign business roles 150
    assign cost center 148
    assign department 148
    assign extended property 166
    assign location 148
    assign shelf 156
    assign system role 154
    assign user account 152
    calculated license 186
    category 146, 164
    effective 161
    exclude 161
    inherit
        limitation 160
    IT Shop 146
    license 146
    manage 142
    overview 161
    risk index 146
    show authorization object 167
project template 199
provisioning
    member list 54

R
report
    overview of all assignments 192
    revision filter 49
role
    assign business roles 150
    assign cost center 148
    assign department 148
    assign extended property 166
    assign location 148
    assign shelf 156
    assign system role 154
    assign user account 153
    calculated license 186
    category 145, 164
    effective 161
    exclude 161
    inherit
        limitation 160
    IT Shop 145
    license 145
    manage 142
    only synchronize changes 49
    overview 161
    risk index 145
    show authorization object 167
role assignment
    validity period 158
router 8

S
SAP product
    assign account definition 179
    assign subscribable reports 180
schedule
    deactivation 55
schema
    changes 38
    compress 38
    update 38
schema type
    create additional 39
security policies 119
security policy 79
security policy attribute 79
server function 98
special version 80-81, 183
start menu 79
subscribable report 180
synchronization
  accelerate 49
  base object
    create 37
  configuration 35
  configure 21
  connection data 21
  connection parameter 21, 35, 37
different clients 37
extended schema 37
only changes 49
permissions 14
prevent 55
restrict synchronization objects 51
scope 35
start 21
synchronization project
  create 21
target system schema 37
variable 35
variable set 37
workflow 21, 37
synchronization analysis report 55
synchronization configuration
  adapt 35
  customize 37
synchronization direction
  to target system 37
synchronization log 35
synchronization project
  create 21
deviation 55
editing 106
project template 199
synchronization server 8
  configure 18
  editing 94
  install 18
  server function 98
synchronization workflow
  create 21
  set up 37
system 102
  report 191
system connection 21
system measurement 182
  assign license 130
CUA system 130
deputy license 189
determine active license 186
find rating 187
license extension 130
publish license 189
register active license 185

target system managers 99
target system reconciliation 51
telephone 120
template
  IT operating data, modify 67

U
user account
  active license 185, 189
address data 115
administrative user account 108
apply template 67
assign central system 129
assign child system 129
assign employee 107, 132
assign extended property 132
assign group 126
assign profile 126
assign role 127
assign structural profile 128
calculated license 189
category 115, 164
default user account 108
delete 139
department 183
deputys license 189
department address 122
external ID 140
fax number 121
fixed values 123
identity 108, 115
license data 183
lock 63, 131, 137, 139
login data 119
manage 107
manage level 125
measurement data 183
overview form 125
password 91, 119
    notification 93
privileged user account 108, 115
rating 187
reference user 119
retrieve 139
risk index 115
set up 114
SNC name 125
telephone number 120
type 108
user name 115
user account type 76, 119
valid from 158
    format 168
valid until 158
    format 168
validity date
    inherited SAP roles 168
    migration 168