One Identity Manager 9.3

Administration Guide for Connecting to SAP R/3

Copyright 2025 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 website (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/trademark-information.aspx. All other trademarks are the property of their respective owners.

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

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

One Identity Manager Administration Guide for Connecting to SAP R/3
Updated - 06 February 2025, 09:36

For the most recent documents and product information, see Online product documentation.

Contents

Managing SAP R/3 environments **9**
Architecture overview 9
One Identity Manager users for managing SAP R/3 12

Setting up SAP R/3 synchronization **14**
Users and authorizations for synchronizing with SAP R/3 15
Installing the One Identity Manager Business Application Programing Interface 18
Uninstalling BAPI transports 21
Setting up the synchronization server 21
Creating a synchronization project for initial synchronization of an SAP client 25
Special features of synchronizing with a CUA central system 36
Excluding a child system from synchronization 38
Displaying synchronization results 39
Customizing the synchronization configuration 40
How to configure SAP R/3 synchronization 41
Configuring synchronization of different clients 42
Changing system connection settings of SAP clients 43
Editing connection parameters in the variable set 43
Editing target system connection properties 44
Updating schemas 45
Adding other schema types 46
Creating a schema extension file 48
Defining tables 49
Defining functions 52
Defining schema types 53
Speeding up synchronization with revision filtering 57
Restricting synchronization objects using user permissions 58
Post-processing outstanding objects 58
Configuring the provisioning of memberships 61
Configuring single object synchronization 63
Accelerating provisioning and single object synchronization 64
Help for analyzing synchronization issues 65

Disabling synchronization ... 65
Synchronizing single objects ... 66
Ignoring data error in synchronization ... 66
Pausing handling of target system specific processes (Offline mode) ... 67

Basic data for managing an SAP R/3 environment ... 70
Setting up account definitions ... 71
Creating an account definition ... 72
Main data for an account definition ... 73
Creating manage levels ... 75
Main data for manage levels ... 77
Creating a formatting rule for IT operating data ... 78
Collecting IT operating data ... 79
Modify IT operating data ... 80
Assigning account definitions to identities ... 81
Assigning account definitions to departments, cost centers, and locations ... 83
Assigning account definitions to business roles ... 83
Assigning account definitions to all identities ... 84
Assigning account definitions directly to identities ... 84
Assigning account definitions to system roles ... 85
Adding account definitions to the IT Shop ... 85
Assigning account definitions to a target system ... 88
Deleting an account definition ... 88
Editing a server ... 90
Main data for a Job server ... 91
Specifying server functions ... 94
Target system managers ... 96

Basic data for user account administration ... 99
User account types ... 99
External identifier types ... 100
SAP parameters ... 101
Displaying main data of SAP parameters ... 101
General main data of SAP parameters ... 102
Assigning SAP parameters to departments, cost centers, and locations ... 102
Assigning SAP parameters to business roles ... 103

Assigning SAP parameters to system roles ... 104
Editing parameter values for indirect SAP parameter assignment ... 105
Inheritance of parameter values by SAP user accounts ... 107
Printers ... 108
Cost centers ... 109
Start menus ... 109
Companies ... 109
Login languages ... 109
Security policies ... 110
Communication types ... 110
Licenses ... 110
Special versions ... 111
Password policies for SAP user accounts ... 112
Predefined password policies ... 112
Using password policies ... 113
Editing password policies ... 115
General main data of password policies ... 115
Policy settings ... 116
Character classes for passwords ... 117
Custom scripts for password requirements ... 119
Checking passwords with a script ... 119
Generating passwords with a script ... 120
Password exclusion list ... 121
Checking a password ... 122
Testing password generation ... 122
Initial password for new SAP user accounts ... 123
Email notifications about login credentials ... 123

SAP systems ... 126

SAP clients ... 127
General main data of SAP clients ... 127
Specifying categories for inheriting SAP groups, SAP roles, and SAP profiles ... 129
Editing synchronization projects ... 130

SAP user accounts ... 131
Linking user accounts to identities ... 132

Supported user account types ... 133
Central user administration in One Identity Manager ... 136
Entering main data of SAP user accounts ... 138
General main data of an SAP user account ... 139
Work center data for SAP user accounts ... 144
SAP user account login data ... 144
Phone numbers ... 146
Fax numbers ... 147
Email addresses ... 148
Fixed values for an SAP user account ... 149
Measurement data ... 150
SNC data for an SAP user account ... 150
Directly assigning SAP parameters ... 150
Additional tasks for managing SAP user accounts ... 151
Overview of SAP user accounts ... 151
Changing the manage level of SAP user accounts ... 152
Assigning SAP groups and SAP profiles directly to an SAP user account ... 152
Assigning SAP roles directly to an SAP user account ... 153
Assigning structural profiles ... 154
Granting access to clients of a central user administration ... 155
Assigning SAP licenses ... 156
Locking and unlocking SAP user accounts ... 158
Assigning extended properties to SAP user accounts ... 158
Renaming SAP user accounts ... 159
Assigning identities automatically to SAP user accounts ... 160
Editing search criteria for automatic identity assignment ... 162
Automatically creating departments based on SAP user account information ... 165
Locking SAP user accounts ... 166
Deleting and restoring SAP user accounts ... 167
Entering external user IDs for SAP user accounts ... 169

SAP groups, SAP roles, and SAP profiles ... 171
Editing main data of SAP groups, SAP roles, and SAP profiles ... 171
General main data of SAP groups ... 172
General main data of SAP roles ... 174
General main data of SAP profiles ... 175

Assigning SAP groups, SAP roles, and SAP profiles to SAP user accounts 177
Assigning SAP groups, SAP roles, and SAP profiles to organizations 178
Assigning SAP groups, SAP roles, and SAP profiles to business roles 180
Assigning SAP user accounts directly to SAP groups and SAP profiles 182
Assigning SAP user accounts directly to SAP roles 183
Adding SAP groups, SAP roles, and SAP profiles to system roles 184
Adding SAP groups, SAP roles, and SAP profiles to the IT Shop 186
Assignment and inheritance of SAP profiles and SAP roles to SAP user accounts 188
Configuring single role assignment 189
Inheriting SAP profiles and SAP roles in a central user administration 190
Additional tasks for managing SAP groups, SAP roles, and SAP profiles 190
Overview of SAP groups, SAP roles, and SAP profiles 190
Effectiveness of SAP groups, SAP roles, and SAP profiles 191
SAP group, SAP role, and SAP profile inheritance based on categories 194
Assigning extended properties to SAP groups, SAP roles, and SAP profiles 196
Showing SAP authorizations 197
Validity period of role assignments 197
Assigning the validity period of direct role assignments 198
Configuring the validity period of indirect role assignments 199
Determining the validity period of indirect role assignments 200

SAP products 202
General main data of SAP products 203
Assigning SAP products to identities 204
Assigning SAP products to organizations 206
Assigning SAP products to business roles 206
Assigning SAP products directly to identities 207
Adding SAP products to system roles 207
Adding SAP products to the IT Shop 208
Additional tasks for managing SAP products 210
Overview of SAP products 210
Assigning SAP groups, SAP roles, and SAP profiles to an SAP product 210
Assigning SAP parameter to SAP products 211
Assigning account definitions to SAP products 212
Assigning subscribable reports to SAP products 212
Assigning extended properties to SAP products 213

Editing conflicting system roles ... 213

Providing system measurement data ... 215

Mapping the measurement data ... 216

Entering licenses for SAP user accounts ... 218

Finding licenses using SAP roles and SAP profiles ... 219

Determining an SAP user account rating ... 220

Transferring calculated licenses ... 222

Disabling license calculation ... 223

Reports about SAP objects ... 225

Overview of all assignments ... 227

Removing a Central User Administration ... 229

Release child systems ... 230

Converting the central system ... 231

Checking for successful conversion ... 233

Troubleshooting an SAP R/3 connection ... 235

Table accesses not performed correctly ... 235

Appendix: Configuration parameters for managing an SAP R/3 environment ... 236

Appendix: Default project templates for synchronizing an SAP R/3 environment ... 240

Project template for client without CUA ... 240

Project template for the CUA central system ... 241

Project template for CUA subsystems ... 243

Appendix: Referenced SAP R/3 table and BAPI calls ... 244

Appendix: Example of a schema extension file ... 248

About us ... 251

Contacting us ... 251

Technical support resources ... 251

Index ... 252

Managing SAP R/3 environments

One Identity Manager offers simplified user administration for SAP R/3 environments. 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 identities with the necessary user accounts. There are different ways for you to connect identities to their user accounts. You can also manage user accounts independently of identities and thus set up administrator user accounts.

Groups, roles, and profiles are mapped in 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 identities. One Identity Manager ensures that the right group memberships are created for the identity'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 for or withdrawn from user accounts in One Identity Manager.

Architecture overview

In One Identity Manager, the following servers play a role in managing SAP R/3:

- SAP R/3 application server

  Application server on which synchronization is run The synchronization server connects to this server in order to access SAP R/3 objects.

- SAP R/3 database server

  Server on which the SAP R/3 application database is installed.

- Synchronization server

  The synchronization server for synchronizing data between One Identity Manager and SAP R/3. The One Identity Manager Service with the SAP R/3 connector is

installed on this server. 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 SAP R/3 One Identity Manager connector runs 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 3.1 for 64-bit for communicating with the target system.

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

Figure 1: Architecture for synchronization - Direct communication

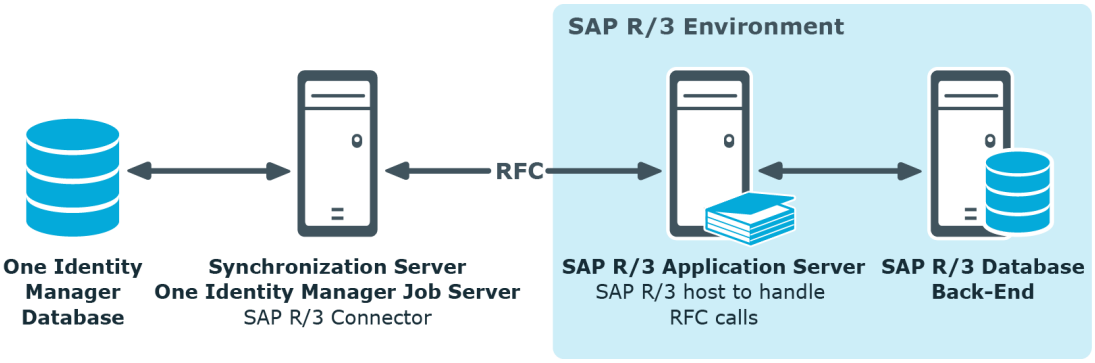


Figure 2: Architecture for synchronization - Communication through message server

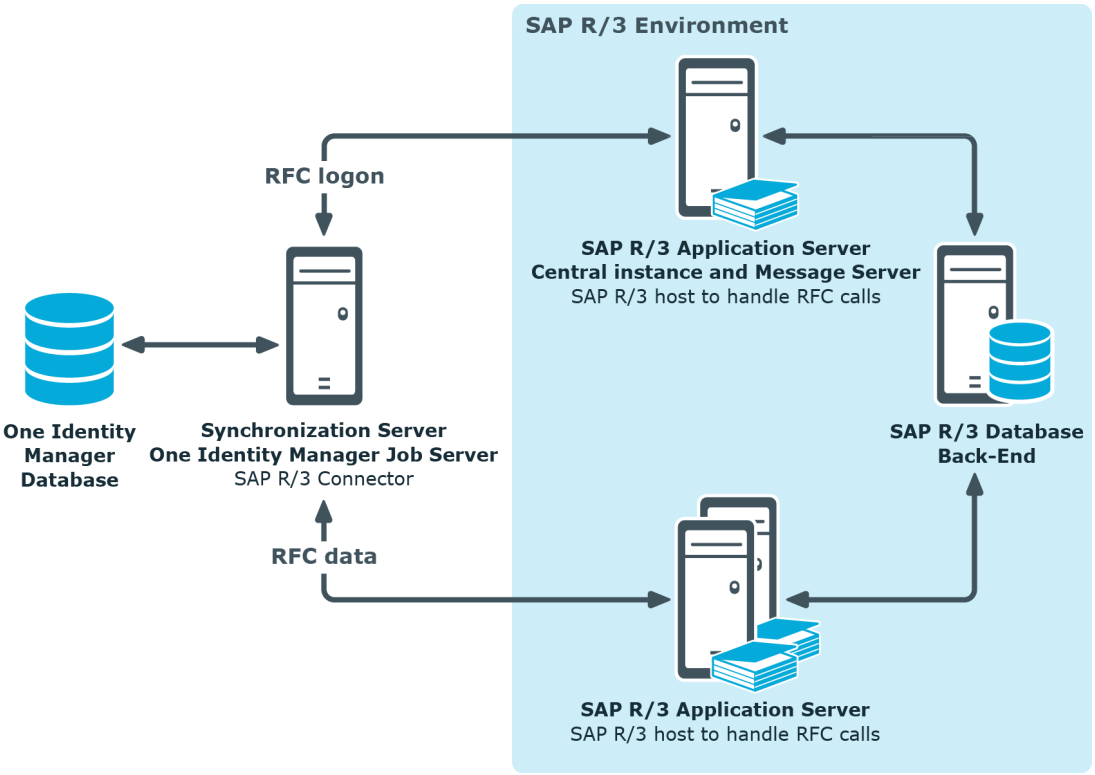
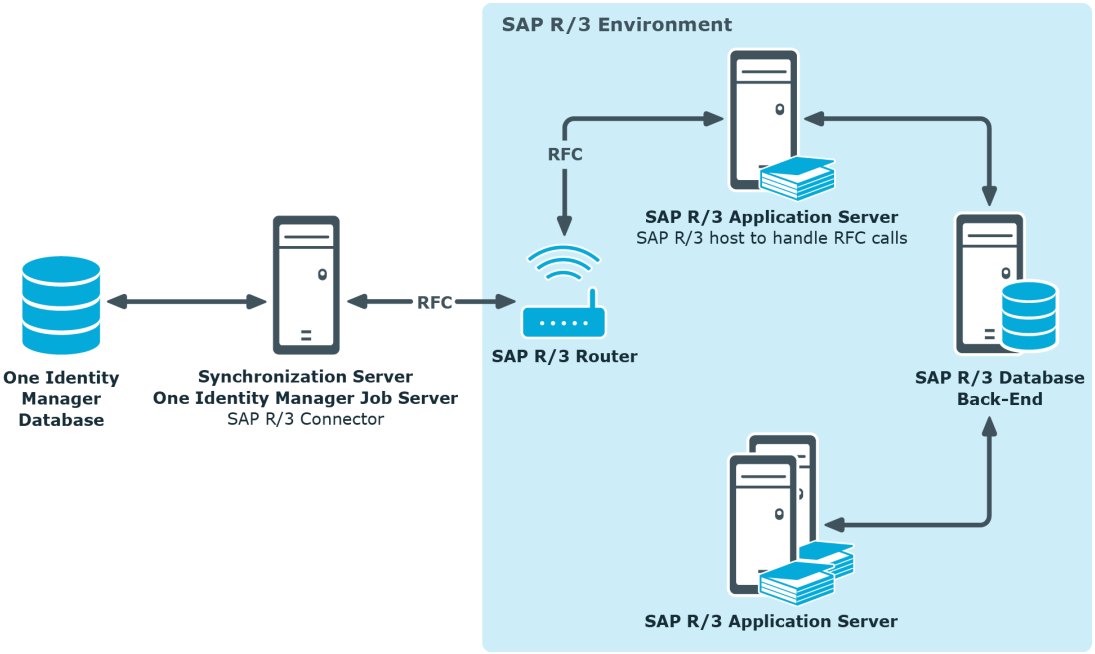


Figure 3: Architecture for synchronization - Communication through router



One Identity Manager users for managing SAP R/3

The following users are used for setting up and administration of SAP R/3.

Table 1: Users

Users	Tasks
Target system administrators	Target system administrators must be assigned to the **Target systems | Administrators** application role. Users with this application role: • Administer application roles for individual target system types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles for target system managers are mutually exclusive. • Authorize other identities to be target system administrators. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the **Target systems | SAP R/3** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects. • Edit password policies for the target system. • Prepare system entitlements to add to the IT Shop. • Can add identities that do not have the **Primary identity** identity type. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other identities within their area of responsibility as target system managers and create child

Users	Tasks
	application roles if required.
One Identity Manager administrators	One Identity Manager administrator and administrative system users Administrative system users are not added to application roles. One Identity Manager administrators: • Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the 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 **Identity Management | Organizations | Administrators** application role. Users with this application role: • Assign system entitlements to departments, cost centers, and locations.
Business roles administrators	Administrators must be assigned to the **Identity Management | Business roles | Administrators** application role. Users with this application role: • Assign system entitlements to business roles.

Setting up SAP R/3 synchronization

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, 7.40 SR 2, 7.41, 7.50, 7.51, 7.52, 7.53, 7.54, 7.55, 7.56, 7.57, 7.58, and 7.69
- SAP ECC 5.0 and 6.0
- SAP S/4HANA On-Premise Edition 1.0 and 2.0 as from SAP BASIS 7.40 SR 2 and 7.50 (also for installations with SAP BASIS 7.53)
- SAP S/4HANA Cloud 2022 and 2023 with SAP BASIS 7.57 and 7.58

Central User Administration is supported for all versions named here.

NOTE: The application server ABAP must be installed as a prerequisite for synchronization. An SAP R/3 system that is only based on a Java application server cannot be accessed with the SAP connector.

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. One Identity Manager components for managing SAP R/3 environments are available if the **TargetSystem | SAPR3** configuration parameter is set.
    - In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.

      NOTE: If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

- 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 Connector for Microsoft .NET 3.1 for Windows 64bit with at least version 3.1.5 (compiled for .NET (formerly .NET Core)).
5. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.
6. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- Users and authorizations for synchronizing with SAP R/3 on page 15
- Installing the One Identity Manager Business Application Programing Interface on page 18
- Setting up the synchronization server on page 21
- Creating a synchronization project for initial synchronization of an SAP client on page 25

Users and authorizations for synchronizing with SAP R/3

The following users play a role in synchronizing One Identity Manager with SAP R/3.

One Identity Manager Service user account

The user account for the One Identity Manager Service requires user permissions to carry out operations at file level (adding 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 permissions.

The user account requires permissions for the internal web service.

NOTE: If the One Identity Manager Service runs under the network service (**NT Authority\NetworkService**), you can grant permissions 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 One Identity Manager.

The default installation installs One Identity Manager under `%ProgramFiles%\One Identity`

User for accessing the One Identity Manager database

The **Synchronization** default system user is provided to run synchronization using an application server.

User for accessing the target system (synchronization user)

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.

Required authorization objects and their meanings:

- S_TCODE with a minimum of transaction codes SU01, SU53, PFCG
- S_ADDRESS1 (address services) with activities 01, 02, 03, 06 and valid address groups (at least BC01)
- S_USER_AGR (role maintenance) with activities 02, 03, 22, 78, possibly with a restricted name range (for example Z*)
- S_USER_GRP (group maintenance) with activities 01, 02, 03, 05, 22, 78 and PP (if available in the SAP R/3 environment)
- S_USER_AUT (authorizations) with activities 03, 08
- S_USER_PRO (profile) with activities 01, 02, 03, 22
- S_USER_SAS (system specific assignments) with activities 01, 06, 22
- S_USER_UID with the activity 03
- 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, SDIFRUNTIME, SYSU,
- /VIAENET/ZVIL_TABLE

  NOTE:

  As of One Identity Manager version 8.2, an updated BAPI transport `SAPTRANSPORT_70.ZIP` is provided. This uses the `/VIAENET/READTABLE` function module instead of the `RFC_READ_TABLE` SAP module. When it accesses an SAP R/3 system, the SAP R/3 connector checks whether the `/VIAENET/READTABLE` function module exists and uses that.

  If the function module is not available, the connector uses the `RFC_READ_TABLE` SAP module.

  In this case, the synchronization user needs the authorization object S_TABU_NAM with the activity 03.

  Alternatively you can define access permissions on the tables using the S_TABU_NAM or the S_TABU_DIS authorization object. These are tested equally.

  In the `TABLE` field, the names of the tables to be read can be specified individually.

Apart from the authorizations listed, the user account must obtain all the authorizations from the ZVIH_AUT, ZVIA_AUT, and ZVIL_AUT authorization objects that are installed by the transport package. These authorization objects are there to guarantee principal authorization for running function modules.

In addition, the authorization objects ZVIH_OP, ZVIA_OP, ZVIL_OP need to be assigned. This regulates the type of access to SAP R/3 data using the ACTVT authorization field. Possible values are **01 add or create**, **02 change**, **03 display**, **06 delete**. The respective activity is checked before accessing data. If only the **03 display** activity has been assigned, it means that absolutely no write operations can be carried out with this user account using the One Identity Manager Business Application Programing Interface.

The following authorization objects are required in addition for the child system in order to synchronize central user administration:

- S_RFC with the function group SUU6
- S_TCODE with the transaction code SU56

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 the `Modules\SAP\dvd\AddOn\Bapi` directory.

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 is permitted, set up a profile that has authorizations for carrying out for transactions SU01 and PFCG but prevents write access at activity or field level. Also be aware of granting authorizations for activities regarding the authorization objects ZVIH_OP, ZVIA_OP, ZVIL_OP. If access is read-only, only the **03 display** activity is enabled.

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. Passwords are 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 Connector for Microsoft .NET), 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 Connector for Microsoft .NET 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

- Referenced SAP R/3 table and BAPI calls on page 244
- Table accesses not performed correctly on page 235

Installing the One Identity Manager Business Application Programing Interface

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

Certificates:

- SAP S/4HANA Cloud Private Edition, release 2023
- Integration with SAP S/4HANA
- Powered by SAP NetWeaver

For more information, see SAP Certified Solutions Directory.

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 the `Modules\SAP\dvd\AddOn\Bapi` directory.

Table 2: BAPI transport

Transport	Explanation
SAPRepository.zip	Imports the /VIAENET/ namespace in to the SAP system repository.
SAPTable.zip	Defines the table structure for /VIAENET/USERS in the SAP system dictionary.
SAPTRANSPORT_70.ZIP	Contains the functions defined in the /VIAENET/ namespace. Select the transport package that suits your SAP system. • Archive directory UNICODE: Transports for systems that support unicode; transports for copies • Archive directory NON_UNICODE: Transports for systems not supporting unicode • Archive directory UNICODE_WORKBENCH: Transports for systems that support unicode; workbench transports • Archive directory NON_UNICODE_WORKBENCH: Transports for systems that do not support unicode; workbench transport

Transport	Explanation
SAPBusinesspartnerProxies.zip	Contains the functions defined in the /VIAENET/HELPER package. The transport is only required if an SAP S/4HANA system is connected and you want to map business partner data associated with SAP user accounts. Select the transport package that suits your SAP system. • Archive directory UNICODE: Transports for systems that support unicode; transports for copies • Archive directory UNICODE_WORKBENCH: Transports for systems that support unicode; workbench transports
SAPAuthorization.zip	Imports all authorization objects defined in the /VIAENET/ namespace as a workbench transport. The transport package contains only the authorization objects from the complete `SAPTRANSPORT_70.ZIP` transport package. Install this transport package if: • You want to test whether these authorization objects can cause issues in your SAP R/3 system or • If you install the assembly kit package `T070020759523_0000019.PAT`.
SAPRole.zip	Contains a transport with an SAP role with all necessary authorizations for the synchronization user.
T070020759523_0000019.PAT	Contains the functions defined in the /VIAENET/ namespace. It does not contain any authorization objects. This means that the `SAPAuthorization.zip` transport must be installed beforehand. The kit has the `deinstall_allowed` option set.

Along with this, the SAP R/3 connector uses other functions of the SAP R/3 system.

Set the following import options for the transport:

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

You might want to install the BAPI transports in a different order depending on your installation scenario.

Installation scenario 1: All objects together

The SAPTRANSPORT_70.ZIP transport file contains all the objects required for the namespace, the table structure, and the functions in the /VIAENET/ namespace.

Installation sequence:

1. SAPTRANSPORT_70.ZIP
2. (Optional) SAPBusinesspartnerProxies.zip
3. (Optional) SAPRole.zip

Installation scenario 2: SAP Add-On Assembly Kit

The SAP Add-On Assembly Kit allows SAP to support uninstalling of a BAPI. An uninstallable Assembly Kit package is provided for this.

Installation sequence:

1. SAPAuthorization.zip
2. T070020759523_0000019.PAT assembly kit package.
3. (Optional) SAPBusinesspartnerProxies.zip
4. (Optional) SAPRole.zip

Installation scenario 3: Separate transports for the namespace and the table structure

The /VIAENET/ namespace and the table structure can be created using separate transports. This allows you to check step by step whether the transports have been successfully installed.

Installation sequence:

1. SAPRepository.zip

   Check whether the /VIAENET/ namespace is available in the SAP system.
2. SAPTable.zip

   Check whether the table structure for /VIAENET/USERS is defined.
3. SAPAuthorization.zip

   Check whether the authorization objects are available.
4. SAPTRANSPORT_70.ZIP

   Check whether all functions defined in the /VIAENET/ namespace are available.
5. (Optional) SAPBusinesspartnerProxies.zip

   Check whether the functions defined in the /VIAENET/HELPER package are available.
6. (Optional) SAPRole.zip

   Assign this role to the user account for the synchronization user.

Related topics

- Referenced SAP R/3 table and BAPI calls on page 244
- Uninstalling BAPI transports on page 21

Uninstalling BAPI transports

The SAP Add-On Assembly Kit allows SAP to support uninstalling of a BAPI. An uninstallable Assembly Kit package is provided for this.

The `T070020759523_0000019.PAT` package can be found on the One Identity Manager installation medium in the `Modules\SAP\dvd\AddOn\Bapi` directory.

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 be able to uninstall a BAPI transport at a later date, install the transports as described in installation scenario 2. For more information, see Installing the One Identity Manager Business Application Programing Interface on page 18.

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

  The following versions are supported:

  - Windows Server 2025
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
- .NET 8 Desktop Runtime

  NOTE: Take the target system manufacturer's recommendations into account.
- Windows Installer

- SAP Connector for Microsoft .NET 3.1 for Windows 64bit with at least version 3.1.5 (compiled for .NET (formerly .NET Core))
- 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 **Server | Job Server | SAP R/3** machine role.

All One Identity Manager Service actions are run 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 recommended that you set up a Job server for each target system for performance reasons. 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).

To set up a Job server, perform the following steps.

1. Create a Job server and install and configure the One Identity Manager Service.

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

   - Sets up a Job server.
   - Specifies machine roles and server function for the Job server.
   - Installs One Identity Manager Service components corresponding to the machine roles.
   - Configures the One Identity Manager Service.
   - Starts the One Identity Manager Service.

   Use the Server Installer to install the One Identity Manager Service locally or remotely.

   To remotely install the One Identity Manager Service, provide an administrative workstation on which the One Identity Manager components are installed. Ensure that the One Identity Manager components are installed on the server before installing locally. For more information about installing One Identity Manager components, see the *One Identity Manager Installation Guide*.
2. If you are working with an encrypted One Identity Manager database, declare the database key in the One Identity Manager Service. For more information about working with an encrypted One Identity Manager database, see the *One Identity Manager Installation Guide*.
3. To generate processes for the Job server, you need the provider, connection parameters and the authentication data. By default, this information is determined from the database connection data. If the Job server runs through an application server, you must configure extra connection data in the Designer. For more information about connection data, see the *One Identity Manager Configuration Guide*.

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

1. Start the Server Installer program.

   NOTE: To install remotely, start the Server Installer program on your administrative workstation. To install locally, start the program on the server.

2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager database.

   You can connect via the application server or directly to connect to the database.

3. On the **Server properties** page, specify the server on which you want to install the One Identity Manager Service.

   a. Select a Job server from the **Server** drop-down.

      - OR -

      To create a new Job server, click **Add**.

   b. Enter the following data for the Job server.

      - **Server**: Name of the Job server.
      - **Queue**: Name of the queue to handle the process steps. Each Job server within the network must have a unique queue identifier. The process steps are requested by the Job queue using this exact queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
      - **Full server name**: Full server name in accordance with DNS syntax.

        Syntax:

        `<Name of servers>.<Fully qualified domain name>`

   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 the Designer.

4. On the **Machine roles** page, select **SAP R/3**.
5. On the **Server functions** page, select **SAP R/3 connector**.
6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

   NOTE: The initial service configuration is predefined. If further changes need to be made to the configuration, you can do this later with the Designer. For more information about configuring the service, see the *One Identity Manager Configuration Guide*.

   For a direct connection to the database:

   a. In the module list, select **Process collection > sqlprovider**.
   b. Click the **Connection parameter** entry, then click the **Edit** button.
   c. Enter the connection data for the One Identity Manager database.
   d. Click **OK**.

For a connection to the application server:

a. In the module list, select the **Process collection** entry and click the **Insert** button.

b. Select **AppServerJobProvider** and click **OK**.

c. In the module list, select **Process collection > AppServerJobProvider**.

d. Click the **Connection parameter** entry, then click the **Edit** button.

e. Enter the address (URL) for the application server and click **OK**.

f. Click the **Authentication data** entry and click the **Edit** button.

g. In the **Authentication method** dialog, select the authentication module for logging in. Depending on the authentication module, other data may be required, such as user and password. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

h. Click **OK**.

7. To configure the installation, click **Next**.
8. Confirm the security prompt with **Yes**.
9. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.
10. On the **Service access** page, enter the service's installation data.

    - **Computer**: Select the server, on which you want to install and start the service, from the drop-down or enter the server's name or IP address.

      To run the installation locally, select `Local installation` from the drop-down.

    - **Service account**: Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

    The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options.

    You can also change the One Identity Manager Service details, such as the installation directory, name, display name, and the One Identity Manager Service description, using the advanced options.
11. Click **Next** to start installing the service.

    Installation of the service occurs automatically and may take some time.
12. Click **Finish** on the last page of the Server Installer.

    NOTE: In a default installation, the service is entered in the server's service management with the name **One Identity Manager Service**.

Creating a synchronization project for initial synchronization of an SAP client

Use the 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 3: Information required for setting up a synchronization project

Data	Explanation
SAP R/3 application server	Name of the application server used to RFC communication.
System number	Number of the SAP system for connecting the SAP R/3 connector.
System ID	System ID of this SAP system.
Client	Number of the client to be synchronized. You need the central system's client number to synchronize central user administration (CUA).
Login name and password	The name and password of the user account used by the SAP R/3 connector to log in to the SAP R/3 system. Make a user account available with sufficient permissions. If the network connection must be secure, you require the user account's SNC name.
Login language	Login language for logging the SAP R/3 connection into the SAP R/3 system.
Synchronization server	All One Identity Manager Service actions are run 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. Installed components: • SAP Connector for Microsoft .NET 3.1 for Windows 64bit with at least version 3.1.5 (compiled for .NET (formerly .NET Core)) • One Identity Manager Service (started)

<table>
<tr><th>Data</th><th>Explanation</th></tr>
<tr><td></td><td>

Synchronization Editor
SAP R/3 connector

The synchronization server must be declared as a Job server in One Identity Manager. Use the following properties when you set up the Job server.
Table 4: Additional properties for the Job server
<table>
<tr><th>Property</th><th>Value</th></tr>
<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>
</table>
For more information, see Setting up the synchronization server on page 21.
</td></tr>
<tr><td>One Identity Manager database connection data</td><td>

Database server
Database name
SQL login and password
Specifies whether integrated Windows authentication is used
Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.

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

One Identity Manager Service is started
RemoteConnectPlugin is installed and an authentication method is set up
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.
</td></tr>
</table>

Data	Explanation
	TIP: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements). Use the synchronization server as remote connection server as well by installing the RemoteConnectPlugin. 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 5: Information for setting up a synchronization project

Data	Explanation
SAP R/3 router	Name of the router that provides a network port for the SAP R/3 connector for communicating with the application server.
SAP R/3 message server	Name of the message server with which the SAP R/3 connector communicates when logging in.
Login group	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.
SNC host name	SNC name of the host for the secure network connection.
SNC Name	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.
SNC client API	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 through 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).

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

- Run in default mode
- Started from the Launchpad

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

NOTE: Just one synchronization project can be created per target system and default project template used.

To set up an initial synchronization project for an SAP client

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

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

2. In the **Installation overview > Data synchronization** section, select the **Target system type SAP R/3** and click **Run**.

   This starts the Synchronization Editor's project wizard.

3. On the wizard's start page, click **Next**.
4. 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 the Synchronization Editor, do not change any settings.
   - If access is not possible from the workstation on which you started the Synchronization Editor, you can set up a remote connection.

     Select the **Connect using remote connection server** and enter the remote connection properties.

     Remote connection properties

     - **Access parameters**
       - **Server**: Full server name or IP address of the server.

         To select an existing Job server as the remote connection server, click and select the server from the drop-down. This displays all the Job servers that have the **One Identity Manager Service installed** server function selected.
       - **Port**: Port that is configured for the RemoteConnectPlugin.
     - **Authentication**

       If **SecretAuthentication** is configured for the RemoteConnectPlugin:

       - **Secret**: Secret used by the Synchronization Editor to authenticate on the RemoteConnectPlugin.

       If **ADGroupAuthentication** is configured for the RemoteConnectPlugin, no data is required.

- **Options**
  - **Request timeout**: Maximum time allowed for a server query in seconds. If the time is exceeded, the request is canceled.
  - **Accept self-signed certificates**: Specifies whether self-signed certificates can be accepted.

5. Select a connection type on **Connection type**.

Table 6: Connection type

Property	Description
SAP R/3 application server or SAP R/3 router	Specifies whether the connection is established through an application server or a router.
SAP R/3 message server	Specifies whether the connection is established over a messaging server.

- On the **Connection data** page, enter the connection data for **SAP R/3 application server or SAP R/3 router** connection type.

Table 7: System connection

Property	Description
SAP R/3 host or router	Name of the application server or router used by the SAP R/3 connector to communicate.
System number	Number of the SAP system.
System ID	The SAP system ID. This is used as the display name in One Identity Manager tools.

- On the **Message server** page, enter the connection data for the **SAP R/3 Message Server** connection type.

Table 8: System connection

Property	Description
SAP R/3 message server	Name of the message server used to establish the connection.
Logon group	Name of the login group that the SAP R/3 connection logs on to.
SAP R/3 router	Name of the router if a router is used by the SAP R/3 connector to communicate.

Property	Description
System number	Number of the SAP system.
System ID	The SAP system ID. This is used as the display name in One Identity Manager tools.

6. Enter the network settings on **Secure network communication**.

Table 9: Network settings

Property	Description
Program ID	Identifies the connection that the SAP R/3 connector establishes with the SAP R/3 system.
SNC logon	Specifies whether the SNC user account name is used when the SAP R/3 connector logs in on the SAP R/3 system. NOTE: In this case, when new user accounts are being provisioned, the effective passwords are only set if single sign-on is used to login.

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

Table 10: SNC system connection

Property	Description
Client	Number of the client to be synchronized. Enter the central system's client number if central user administration is to be synchronized.
SNC host name	SNC name of the host for the secure network connection.
SNC name	The name of the user account used by the SAP R/3 connector to log in to the SAP R/3 system.
SNC client API	API containing the SNC encryption.
Authentication	Select a security level for logging in to the SAP R/3 system.
Integrity protection	
Encryption	
Highest available level	

Property	Description
SNC login with user name and password	User name and password are given explicitly during SNC login. In this case, no production passwords can be set when provisioning new user accounts. If this option is not set, single sign-on is used for logging in. In this case, the production passwords are set when provisioning new user accounts.
Login language	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 **EN**, all texts from SAP groups, roles, profiles, and start menus are synchronized in English.

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

   This page is shown if you have not set the **SNC login** option on the **Secure connection** page or if you have set the **SNC login using username/password** option on the **SNC connection data** page.

   Table 11: Login data

Property	Description
Client	Number of the client to be synchronized. Enter the central system's client number if central user administration is to be synchronized.
Login name	The 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 **SNC login** on the **Secure connection** page, enter the SNC name of this user account.
Login password	The user account's password used by the SAP R/3 connector to log in to the SAP R/3 system.
Login language	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 **EN**, all texts from SAP groups, roles, profiles, and start menus are synchronized in English.

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 to see if the supplied BAPI is installed.

- Click **Finish**, to end the system connection wizard and return to the project wizard.

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 46.

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. On the **Select project template** page, select a project template to use for setting up the synchronization configuration.

Table 12: Standard project templates

Project template	Description
SAP R/3 Synchronization (Basic Administration)	Use this project template for the initial setup of the synchronization project for individual clients or the central system of a CUA.
SAP R/3 (CUA subsystem)	Use this project template for the initial setup of the synchronization project for child systems of a CUA that belong to a different SAP system than the central system.

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, specify how system access should work. You have the following options:

Table 13: Specify target system access

Option	Meaning
Read-only access to target system.	Specifies that a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database. The synchronization workflow has the following characteristics: • Synchronization is in the direction of `One Identity Manager`. • Processing methods in the synchronization steps are only defined for synchronization in the direction of `One Identity Manager`. NOTE: If you initially select this option, no write operations are possible in the target system. If you want to use this synchronization project later to publish changes to the target system, you have two options: a. Manually configure all required elements of the synchronization configuration (mapping, workflows and others). - OR - b. Create a new synchronization project to replace the previous one. Note that only one synchronization project can be set up for each base object.
Read/write access to target system. Provisioning available.	Specifies whether a provisioning workflow is set up in addition to the synchronization workflow for the initial loading of the target system. The provisioning workflow displays the following characteristics: • Synchronization is in the direction of the `Target system`. • Processing methods are only defined in the synchronization steps for synchronization in the direction of the `Target system`. • Synchronization steps are only created for such schema classes whose schema types have write access.

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. On the **Synchronization server** page, select the synchronization server to run the synchronization.

    If the synchronization server is not declared as a Job server for this target system 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.

    > TIP: You can also implement an existing Job server as the synchronization server for this target system.
    >
    > - To select a Job server, click .
    >
    > This automatically assigns the server function matching this Job server.

    c. Click **OK**.

    The synchronization server is declared as Job server for the target system in the One Identity Manager database.

    d. > 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.

    This sets up, saves and immediately activates the synchronization project.

    > NOTE:
    >
    > - If enabled, a consistency check is carried out. If errors occur, a message appears. You can decide whether the synchronization project can remain activated or not.
    >
    >   Check the errors before you use the synchronization project. To do this, in the **General** view on the Synchronization Editor's start page, click **Verify project**.
    > - 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.
    > - The connection data for the target system is saved in a variable set and can be modified in the Synchronization Editor in the **Configuration > Variables** category.

To configure the content of the synchronization log

1. In the Synchronization Editor, open the synchronization project.
2. To configure the synchronization log for target system connection, select the **Configuration > Target system** category.
3. To configure the synchronization log for the database connection, select the **Configuration > One Identity Manager connection** category.
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 error analysis and other analyzes.
7. Click **OK**.

To synchronize on a regular basis

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Start up configurations** category.
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. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Start up configurations** category.
3. Select a start up configuration in the document view and click **Run**.
4. Confirm the security prompt with **Yes**.

NOTE:

In the default installation, after synchronizing, identities are automatically created for the user accounts.If an account definition for the client is not known at the time of synchronization, user accounts are linked with identities. 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 manage user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the client.

3. Assign a user account in the **Linked** state to the account definition. The account definition's default manage level is applied to the user account.
    a. In the Manager, select the **SAP R/3 > User accounts > Linked but not configured > <client>** category.
    b. Select the **Assign account definition to linked accounts** task.
    c. In the **Account definition** drop-down, select the account definition.
    d. Select the user accounts that contain the account definition.
    e. Save the changes.

Detailed information about this topic

- One Identity Manager Target System Synchronization Reference Guide

Related topics

- Setting up the synchronization server on page 21
- Users and authorizations for synchronizing with SAP R/3 on page 15
- Displaying synchronization results on page 39
- Customizing the synchronization configuration on page 40
- Speeding up synchronization with revision filtering on page 57
- Default project templates for synchronizing an SAP R/3 environment on page 240
- Setting up account definitions on page 71
- Assigning identities automatically to SAP user accounts on page 160
- Adding other schema types on page 46

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 run 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.

When a comparison of role and profile text is carried out between the child and the central system in the target system, roles and profiles are saved in USRSYSACTT with respect to language. 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 25. The following special features apply:

   1. In **Select project template** in the project wizard, select the "SAP R/3 (CUA subsystem)" project template.
   2. The **Restrict target system access** page is not displayed. The target system is only loaded.
   3. 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 25. The following special features apply:

   a. On the **Additional settings** page, enable the **Central User Administration (CUA) instance** option.
   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 main data of SAP clients on page 127
- Excluding a child system from synchronization on page 38

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 the **SAP R/3 > Clients** category.
2. Select the child system in the result list. Select the **Change main data** task.
3. Delete the entry in the **ALE model name** field.
4. Save the changes.
5. In the Synchronization Editor, open the synchronization project.
6. Select the **Workflows** category.
7. Select the workflow to use for synchronizing the central system in the navigation view.
8. Double-click on the synchronization step "client" in the workflow view.
9. Select **Rule filter**.
10. Select "ALEModelName_ALEModelName" in the **Exluded rules** pane.
11. Click **OK**.
12. Save the changes.

NOTE: Unsuccessful database operations for assigning SAP roles and profiles to user accounts 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 roles and profiles the moment it becomes part of the central user administration again.

To re-include a child system in synchronization

1. Select the **SAP R/3 > Clients** category.
2. Select the child system in the result list. Select the **Change main data** task.
3. Enter the ALE model name of the central system's CUA in the **ALE model name** field.

   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. In the Synchronization Editor, open the synchronization project.
6. Select the **Workflows** category.
7. Select the workflow in the navigation, to use for synchronizing the central system (default is "Initial Synchronization").
8. Double-click on the synchronization step "client" in the workflow view.
9. Select **Rule filter**.
10. Deselect "ALEModelName_ALEModelName" in the **Exluded rules** pane.
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 main data of SAP clients on page 127

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. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.
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 it.

   An analysis of the synchronization is shown as a report. You can save the report.

To display a provisioning log

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.
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 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 status of the synchronization/provisioning.

TIP: The logs are also displayed in the Manager under the **<target system> > synchronization log** category.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Customizing the synchronization configuration

Having used the Synchronization Editor to set up a synchronization project for initial synchronization of an SAP client, you can use the 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 to be able to regularly compare the database with the SAP R/3 environment and to synchronize changes.

- To use One Identity Manager as the primary system during synchronization, create a workflow with synchronization in the direction of the `Target system`.
- To specify which SAP objects and database objects 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 method, for example.
- Use variables to set up a synchronization project for synchronizing 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 a synchronization process is running, you must not start another synchronization process for the same target system. This especially applies, if the same synchronization objects would be processed.

- If another synchronization process is started with the same start up configuration, the process is stopped and is assigned **Frozen** status. An error message is written to the One Identity Manager Service log file.
  - Ensure that start up configurations that are used in start up sequences are not started individually at the same time. Assign start up sequences and start up configurations different schedules.
- Starting another synchronization process with different start up configuration that addresses same target system may lead to synchronization errors 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 run in sequence.
  - Group start up configurations with the same start up behavior.

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

Detailed information about this topic

- How to configure SAP R/3 synchronization on page 41
- Configuring synchronization of different clients on page 42
- Updating schemas on page 45
- Adding other schema types on page 46
- Changing system connection settings of SAP clients on page 43

How to configure SAP R/3 synchronization

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 primary 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. In the Synchronization Editor, open the synchronization project.
2. Check whether the existing mappings can be used to synchronize into the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.

   This creates a workflow with `Target system` as its direction of synchronization.
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 42

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. In the Synchronization Editor, open the synchronization project.
3. Create a new base object for every other tenant.
   - Use the wizard to attach a base object.
   - In the wizard, select the SAP connector.
   - Declare the connection parameters. The connection parameters are saved in a special variable set.

   A start up configuration is created that 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 SAP R/3 synchronization on page 41

Changing system connection settings of SAP clients

When you set up synchronization for the first time, the system connection properties are set to default values that you can modify. There are two ways to do this:

a. Specify a specialized variable set and change the values of the affected variables.

   The default values remain untouched in the default variable set. The variables can be reset to the default values at any time. (Recommended action).

b. Edit the target system connection with the system connection wizard and change the effected values.

   The system connection wizard supplies additional explanations of the settings. The default values can only be restored under particular conditions.

Detailed information about this topic

- Editing connection parameters in the variable set on page 43
- Editing target system connection properties on page 44

Editing connection parameters in the variable set

The connection parameters were saved as variables in the default variable set when synchronization was set up. You can change the values in these variables to suit you requirements and assign the variable set to a start up configuration and a base object. This means that you always have the option to use default values from the default variable set.

NOTE: To guarantee data consistency in the connected target system, ensure that the start-up configuration for synchronization and the base object for provisioning use the same variable set. This especially applies if a synchronization project is used for synchronizing different SAP clients.

To customize connection parameters in a specialized variable set

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
3. Open the **Connection parameters** view.

   Some connection parameters can be converted to variables here. For other parameters, variables are already created.
4. Select a parameter and click **Convert**.

5. Select the **Configuration > Variables** category.

   All specialized variable sets are shown in the lower part of the document view.
6. Select a specialized variable set or click on in the variable set view's toolbar.
   - To rename the variable set, select the variable set and click the variable set view in the toolbar. Enter a name for the variable set.
7. Select the previously added variable and enter a new value.
8. Select the **Configuration > Start up configurations** category.
9. Select a start up configuration and click **Edit**.
10. Select the **General** tab.
11. Select the specialized variable set in the **Variable set** menu.
12. Select the **Configuration > Base objects** category.
13. Select the base object and click.

    - OR -

    To add a new base object, click .
14. Select the specialized variable set in the **Variable set** menu.
15. Save the changes.

For more information about using variables and variable sets, or restoring default values and adding base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- Editing target system connection properties on page 44

Editing target system connection properties

You can also use the system connection wizard to change the connection parameters. If variables are defined for the settings, the changes are transferred to the active variable set.

NOTE: In the following circumstances, the default values cannot be restored:

- The connection parameters are not defined as variables.
- The default variable set is selected as an active variable set.

In both these cases, the system connection wizard overwrites the default values. They cannot be restored at a later time.

To edit connection parameters using the system connection wizard

1. In the Synchronization Editor, open the synchronization project.
2. In the toolbar, select the active variable set to be used for the connection to the target system.

   NOTE: If the default variable set is selected, the default values are overwritten and cannot be restored at a later time.
3. Select the **Configuration > Target system** category.
4. Click **Edit connection**.

   This starts the system connection wizard.
5. Follow the system connection wizard instructions and change the relevant properties.
6. Save the changes.

Related topics

- Editing connection parameters in the variable set on page 43

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 the loading of 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 compression 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. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.

   - OR -

   Select the **Configuration > One Identity Manager connection** category.
3. Select the **General** view and click **Update schema**.
4. Confirm the security prompt with **Yes**.

   This reloads the schema data.

To edit a mapping

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Mappings** category.
3. Select a mapping in the navigation view.

   Opens the Mapping Editor. For more 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 the **Configuration > Target system** category.
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 ready.

   For more information, see Creating a schema extension file on page 48.
3. Open the synchronization project in the Synchronization Editor.
4. Select the **Configuration > Target system** category.
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 **Mapping** category 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 more 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 worklows. 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 more 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.

NOTE:

As of One Identity Manager version 8.2, an updated BAPI transport `SAPTRANSPORT_70.ZIP` is provided. This uses the `/VIAENET/READTABLE` function module instead of the `RFC_READ_TABLE` SAP module. When it accesses an SAP R/3 system, the SAP R/3 connector checks whether the `/VIAENET/READTABLE` function module exists and uses that.

If the function module is not available, the connector uses the `RFC_READ_TABLE` SAP module.

Schema extension file structure

```
<?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. This includes system variables that are known to the `/VIAENET/READTABLE` function module or the SAP module `RFC_READ_TABLE`.

Table 14: System variable examples

Variable	Description
sy-langu	Currently selected login language.
sy–datum	Current date.
sy-mandant	Current client.

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

Table 15: Predefined SAP R/3connector variables

Variable	Description
$Value$	Input parameter for the One Identity Manager Service call.
$Mandt$	Current client's number.
$Date$	Current date.

Detailed information about this topic

- Defining tables on page 49
- Defining functions on page 52
- Defining schema types on page 53
- Example of a schema extension file on page 248
- Table accesses not performed correctly on page 235

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 requires when it loads the synchronization objects. All columns in the table are loaded when single objects are accessed.

Table 16: Table definition

Attribute	Description
Definition	Symbolic name for using the definition.
TableName	Name of the table in the SAP database.
Key	Key term for formatting the distinguished name. Multiple values can be entered in a comma delimited list.

Attribute	Description
X500	Abbreviation for the key term in the attribute `Key`. Multiple values can be entered in a comma delimited list.
SQL	Limiting WHERE clause. 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 SQL attribute on page 51.
Distinct	Counts the columns that the `Distinct` filter applies to (as comma delimited list).
Load	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. 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 17: Permitted operators in the SQL attribute

Operator	Function/Example
EQ	=
NE	<>
GT	>
LT	<
GE	>=
LE	<=
BETWEEN	ENDDA BETWEEN '20090101' AND '20090131'

- A table definition can also contain a mapping block. This block is used to replace parameters that are supposed to be used in WHERE clauses but were selected with another name in the object list.

  In the example, every occurrence of the $BNAME$ variable was replaced with the current value in the USERNAME column when single objects were loaded from the RSECUSERAUTH table before SQL selection was run. The column USERNAME must be loaded into an object list beforehand.

  Table definitions with a mapping are primarily used to load single objects.
- Predefined variables can be used as well as custom defined parameters in the WHERE clause. For more information, see Creating a schema extension file on page 48.

Example

```
<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>
```

Related topics

- Creating a schema extension file on page 48
- Defining functions on page 52
- Defining schema types on page 53

- Example of a schema extension file on page 248
- Table accesses not performed correctly on page 235

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 18: Function definition

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

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 48. Apart from that, it is possible to pass a fixed value to a function parameter. The following notation is provided for this.

```
<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>
```

Related topics

- Defining tables on page 49
- Defining schema types on page 53
- Creating a schema extension file on page 48
- Example of a schema extension file on page 248

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 `Name` attribute is used as the name. This identifier must be unique in the extended connector schema.

Table 19: Schema type definition

Attribute	Description
Bem	Internal description
Name	Name of the schema type in the extended connector schema.
DisplayPattern	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 (`Key` or `Load` attribute) can be used. If there is no `DisplayPattern` defined, the object's distinguished name is used as the display value. NOTE: The use of multi-value columns (MVP) in the `DisplayPattern` is not allowed 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.
AddRevisionTimeOffset	Specifies whether the revision counter adds the time as **`23:59:00`**. (Optional) You can use this attribute if the revision counter only contains a change date but no timestamp. This allows objects that were changed after the previous synchronization run but on the same day, to be included in the next synchronization run.
RevisionProperty	Name of a property contain the revision counter. (Optional)

Attribute	Description
ListObjectsDefinition	Function or table definition for calling an object list.
ReadObjectDefinition	Function or table definition for calling a single object.
InsertObjectDefinition	Function call to create the new object. (Optional)
InsertCommitDefinition	Function call that should be run after the function to create the new object. (Optional)
WriteObjectDefinition	Function call to write the object. (Optional)
WriteCommitDefinition	Function call that should be run after the function to write the new object. (Optional)
DeleteObjectDefinition	Function call to delete the object. (Optional)
DeleteCommitDefinition	Function call that should be run after the function to delete the object. (Optional)
ParentType	Context of the schema type. (Optional) 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 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.P One single property is defined by the `Property` tag, which can have the following attributes.

Table 20: Property definition

Attribute	Description
Name	Name of the property. It must be unique within the schema type.
Description	Property description.
ListFunction	Function or table for calling all values.

Attribute	Description
AddFunction	Function for adding a value. (Optional)
DelFunction	Function for deleting a value. (Optional)
ReplaceFunction	Replaces the entire contents of the property. (Optional)
IsMultivalued	Specifies whether the property has multiple values. (Optional) If the attribute is not defined, the property is not multi-valued.

Example

```
<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>
    <TABLE Definition = "ANLA-
Table" TableName="ANLA" Key="BUKRS,ANLN1" X500="CN,OU" SQL="MANDT = sy-
mandt" Load="AEDAT" />
</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>
</Functions>
<SAPExtendedSchematypes>
    <SAPExtendedSchematype Bem = "all
users" Name = "UserFunctionTable" DisplayPattern="%BNAME%
(%MANDT%)" RevisionProperty="TRDAT" ListObjectsDefinition = "USR02-Table" ReadOb-
jectDefinition ="USER GET" WriteObjectDefinition = "USER
SET" DeleteObjectDefinition = "USER DEL">
        <Properties>
            <Property Name = "SAPBWP" Description="all BW profiles of the
user" ListFunction="RSECUSERAUTH-
SingleUser" AddFunction="BWProfileAddFkt" DelFunction="BWProfileDelFkt" ReplaceFunction
="" IsMultivalued = "true" />
            <Property Name = "USERPROFILE" Description="all profiles of the
user" ListFunction="USR04-Table" AddFunction="" DelFunction="" ReplaceFunction="USER
PROFILE SET" IsMultivalued = "true" />
        </Properties>
    </SAPExtendedSchematype>
    <SAPExtendedSchematype Bem = "Asset, asset values" Name = "Asset_ANLA" DisplayPat-
tern="%ANLN1% %BUKRS%" AddRevisionTimeOffset="true" RevisionProperty="AEDAT" ListOb-
jectsDefinition = "ANLA-Table" ReadObjectDefinition = "ANLA-
Table" InsertObjectDefinition = "" WriteObjectDefinition = "" DeleteObjectDefinition =
"" />
</SAPExtendedSchematypes>
```

Explanation:

The list of `UserFunctionTable` schema type objects is created by using the `USR02` table. 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 `RSECUSERAUTH` table. 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 (`USER04`) 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 `USR02.BNAME` and

USR04.BNAME columns. There is no mapping required for the table definition because the key columns have the same name.

The Asset_ANLA schema type uses the AESAT revision counter, which only contains a change date. The connector adds a time of **23.59:00** to this revision counter (AddRevisionTimeOffset="true").

Related topics

- Defining tables on page 49
- Defining functions on page 52
- Creating a schema extension file on page 48
- Example of a schema extension file on page 248

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 the last date is was run as a revision in the One Identity Manager database (DPRRevisionStore table, Value column). 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 modified by synchronization are loaded and checked by the next synchronization. This means that the second synchronization after initial synchronization is not significantly faster.

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

To permit revision filtering on a workflow

- In the Synchronization Editor, open the synchronization project.
- Edit the workflow properties. Select the **Use revision filter** item from **Revision filtering** drop-down.

To permit revision filtering for a start up configuration

- In the Synchronization Editor, open the synchronization project.
- Edit the start up configuration properties. Select the **Use revision filter** item from the **`Revision filtering`** drop-down.

Detailed information about this topic

- One Identity Manager Target System Synchronization Reference Guide

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 the authorization check (in the login data).

During synchronization, exactly those groups are read into the One Identity Manager database to which the user account, with which the SAP R/3 connector logs on to the target system, has been granted access in the S_USER_GRP authorization object. All user accounts that are assigned one of these groups as user group for authorization checking, 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 synchronizations.
- 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 the Manager, select the **SAP R/3 > Target system synchronization: SAP R/3** category.

   The navigation view lists all the synchronization tables assigned to the `SAP R/3` target system type.
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 run. 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 from the target system.

     The base object of the assignment was 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.
   - An object that contains a member list has been deleted from the target system.

     During synchronization, the object and all corresponding entries in the assignment tables are marked as outstanding. However, an entry in the synchronization log appears only for the deleted object.

   TIP:

   To display the properties of an outstanding object

   1. Select the object on the target system synchronization form.
   2. Open the context menu and click **Show object**.
   3. For memberships, select the object whose properties you want to display.
3. Select the objects you want to rework. Multi-select is possible.
4. Click on one of the following icons in the form toolbar to run the respective method.

Table 21: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account. Indirect memberships cannot be deleted.
	Publish	The object is added to the target system. The **Outstanding** label is removed from the object. 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.
	Reset	The **Outstanding** label is removed for the object.

TIP: If a method cannot be run due to certain restrictions, the respective icon is disabled.

- To display the constraint's details, click the **Show** button in the **Constraints** column.

5. Confirm the security prompt with **Yes**.

NOTE: By default, the selected objects are processed in parallel, which speeds up 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

- Disable the icon in the form's toolbar.

You must customize your target system synchronization to synchronize custom tables.

To add custom tables to target system synchronization

1. In the Manager, select the **SAP R/3 > Basic configuration data > Target system types** category.
2. In the result list, select the **SAP R/3** target system type.
3. Select the **Assign synchronization tables** task.
4. In the Add assignments pane, assign **custom** tables to the outstanding objects you want to handle.
5. Save the changes.

6. Select the **Configure tables for publishing** task.
7. Select the custom tables that contain the outstanding objects that can be published in the target system and set the **Publishable** option.
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 **Connection is read-only** option must not be set for the target system connection.

Configuring the provisioning of memberships

Memberships, such as 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 may be overwritten. This behavior can occur under the following conditions:

- Memberships are saved as an object property in list form in the target system.

  Example: List of role assignments in the `AGR_NAME` property of an SAP R/3 user (`User`)
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

If one membership in One Identity Manager changes, by default, the complete list of members is transferred to the target system. Therefore, memberships that were previously added to the target system are removed in the process and 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 the Manager, select the **SAP R/3 > Basic configuration data > Target system types** category.
2. In the result list, select the **SAP R/3** target system type.
3. Select the **Configure tables for publishing** task.
4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.
5. Click **Merge mode**.

NOTE:

- This option can only be enabled for assignment tables that have a base table with a `XDateSubItem` column.
- Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically.

6. Save the changes.

For each assignment table labeled like this, the changes made in One Identity Manager are saved in a separate table. Therefore, only newly added and deleted assignments are processed. 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 not the entire members list.

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.

You can restrict single provisioning of memberships with a condition. Once merge mode has been disabled for a table, the condition is deleted. Tables that have had the condition deleted or edited are marked with the following icon: . You can restore the original condition at any time.

To restore the original condition

1. Select the auxiliary table for which you want to restore the condition.
2. Right-click on the selected row and select the **Restore original values** context menu item.
3. Save the changes.

NOTE: To create the reference to the added or deleted assignments in the condition, use the `i` table alias.

Example of a condition on the `SAPUserInSAPGrp` assignment table:

```
exists (select top 1 1 from SAPUser u
     where u.UID_SAPUser = i.UID_SAPUser
     and <limiting condition>)
```

For more 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 `SAPUserInSAPRole` table.

Configuring single object synchronization

Changes made to individual objects in the target system can be immediately applied in the One Identity Manager database without having to start a full synchronization of the target system environment. Individual objects can only be synchronized if the object is already present in the One Identity Manager database. The changes are applied to the mapped object properties. If the object is no longer present in the target system, then it is deleted from the One Identity Manager database.

Prerequisites

- A synchronization step exists that can import the changes to the changed object into One Identity Manager.
- The path to the base object of the synchronization is defined for the table that contains the changed object.

Single object synchronization is fully configured for synchronization projects created using the default project template. If you want to incorporate custom tables into this type of synchronization project, you must configure single object synchronization for these tables. For more information about this, see the *One Identity Manager Target System Synchronization Reference Guide*.

To define the path to the base object for synchronization for a custom table

1. In the Manager, select the **SAP R/3 > Basic configuration data > Target system types** category.
2. In the result list, select the **SAP R/3** target system type.
3. Select the **Assign synchronization tables** task.
4. In the **Add assignments** pane, assign the custom table for which you want to use single object synchronization.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the custom table and enter the **Root object path**.

   Enter the path to the base object in the ObjectWalker notation of the VI.DB.

   Example: `FK(UID_SAPMandant).XObjectKey`
8. Save the changes.

Related topics

- Synchronizing single objects on page 66
- Post-processing outstanding objects on page 58

Accelerating provisioning and single object synchronization

To smooth out spikes in data traffic, handling of processes for provisioning and single object synchronization can be distributed over several Job servers. This will also accelerate these processes.

NOTE: You should not implement load balancing for provisioning or single object synchronization on a permanent basis. Parallel processing of objects might result in dependencies not being resolved because referenced objects from another Job server have not been completely processed.

Once load balancing is no longer required, ensure that the synchronization server runs the provisioning processes and single object synchronization.

To configure load balancing

1. Configure the server and declare it as a Job server in One Identity Manager.
   - Job servers that share processing must have the **No process assignment** option enabled.
   - Assign the **SAP R/3 connector** server function to the Job server.

   All Job servers must access the same SAP client as the synchronization server for the respective base object.
2. In the Synchronization Editor, assign a custom server function to the base object.

   This server function is used to identify all the Job servers being used for load balancing.

   If there is no custom server function for the base object, create a new one.

   For more information about editing base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.
3. In the Manager, assign this server function to all the Job servers that will be processing provisioning and single object synchronization for the base object.

   Only select those Job servers that have the same configuration as the base object's synchronization server.

Once all the processes have been handled, the synchronization server takes over provisioning and single object synchronization again.

To use the synchronization server without load balancing.

- In the Synchronization Editor, remove the server function from the base object.

For more information about load balancing, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- Editing a server on page 90

Help for analyzing synchronization issues

You can generate a report for analyzing problems that arise during synchronization, inadequate performance for example. The report contains information such as:

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

To generate a synchronization analysis report

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Help > Generate synchronization analysis report** menu item and click **Yes** in the security prompt.

   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. In the Synchronization Editor, open the synchronization project.
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. In the Synchronization Editor, open the synchronization project.
2. Select the **General** view on the home page.
3. Click **Deactivate project**.

Detailed information about this topic

- Creating a synchronization project for initial synchronization of an SAP client on page 25
- Pausing handling of target system specific processes (Offline mode) on page 67

Synchronizing single objects

Individual objects can only be synchronized if the object is already present in the One Identity Manager database. The changes are applied to the mapped object properties.

NOTE: If the object is no longer present in the target system, then it is deleted from the One Identity Manager database.

To synchronize a single object

1. In the Manager, select the **SAP R/3** category.
2. Select the object type in the navigation view.
3. In the result list, select the object that you want to synchronize.
4. Select the **Synchronize this object** task.

   A process for reading this object is entered in the job queue.

NOTE: If single object synchronization is run for a user account, the assigned SAP group, roles, profiles, parameters, and communications data are not read in.

To transfer changes to assignments in to One Identity Manager, run a full synchronization.

Detailed information about this topic

- Configuring single object synchronization on page 63

Ignoring data error in synchronization

By default, objects with incorrect data are not synchronized. These objects can be synchronized once the data has been corrected. In certain situations, however, it might be

necessary to synchronize objects like these and ignore the data properties that have errors. This synchronization behavior can be configured in One Identity Manager.

To ignoring data errors during synchronization in One Identity Manager

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > One Identity Manager connection** category.
3. In the **General** view, click **Edit connection**.

   This starts the system connection wizard.
4. On the **Additional options** page, enable **Try to ignore data errors**.

   This option is only effective if **Continue on error** is set in the synchronization workflow.

   Default columns, such as primary keys, UID columns, or mandatory input columns cannot be ignored.
5. Save the changes.

IMPORTANT: If this option is set, One Identity Manager tries to ignore commit errors that could be related to data errors in a single column. This causes the data changed in the affected column to be discarded and the object is subsequently saved again. This effects performance and leads to loss of data.

Only set this option in the exceptional circumstance of not being able to correct the data before synchronization.

Pausing handling of target system specific processes (Offline mode)

If a target system connector is not able to reach the target system temporarily, you can enable offline mode for the target system. This stops target system specific processes from being frozen and having to be manually re-enabled later.

Whether offline mode is generally available for a target system connection is set in the base object of the respective synchronization project. Once a target system is truly unavailable, the target system connection can be switched offline and online again with the Launchpad.

In offline mode, all Job servers assigned to the base object are stopped. This includes the synchronization server and all Job servers involved in load balancing. If one of the Job servers also handles other tasks, these are not processed either.

Prerequisites

Offline mode can only be specified for a base object if certain prerequisites are fulfilled.

- The synchronization server is not used for any other base object as a synchronization server.

- If a server function is assigned to the base object, none of the Job servers with this server function may have any other server function (for example, update server).
- A dedicated synchronization server must be set up to exclusively process the Job queue for this base object. The same applies to all Job servers that are determined by the server function.

To allow offline mode for a base object

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Base objects** category.
3. Select a base object in the document view and click .
4. Enable **Offline mode available**.
5. Click **OK**.
6. Save the changes.

IMPORTANT: To prevent data inconsistencies, the offline phase should be kept as short as possible.

The number of processes to handle depends on the extent of the changes in the One Identity Manager database and their effect on the target system during the offline phase. To establish data consistency between the One Identity Manager database and the target system, all pending processes must be handled before synchronization can start.

Only use offline mode, if possible, for short system downtimes such as maintenance windows.

To flag a target system as offline

1. Start the Launchpad and log in on the One Identity Manager database.
2. Select **Manage > System monitoring > Flag target systems as offline**.
3. Click **Run**.

   This opens the **Manage offline systems** dialog. The **Base objects** section displays the base objects of target system connections that can be switched to offline.
4. Select the base object whose target system connection is not available.
5. Click **Switch offline**.
6. Confirm the security prompt with **OK**.

   This stops all the Job servers assigned to the base object. No more synchronization or provisioning Jobs are performed. The Job Queue Info program shows when a Job server has been switched offline and the corresponding tasks are not being processed.

For more information about offline mode, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- Disabling synchronization on page 65

3

Basic data for managing an SAP R/3 environment

To manage an SAP R/3 environment in One Identity Manager, the following basic data is relevant.

- Configuration parameter

  Use configuration parameters to configure the behavior of the system's basic settings. One Identity Manager provides default settings for various 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. In the Designer, you can find an overview of all configuration parameters in the **Base data > General > Configuration parameters** category.

  For more information, see Configuration parameters for managing an SAP R/3 environment on page 236.

- Account definitions

  One Identity Manager has account definitions for automatically allocating user accounts to identities. You can create account definitions for every target system. If an identity 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 identity.

  For more information, see Setting up account definitions on page 71.

- Password policy

  One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the identities' 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 use or customize if required. You can also define your own password policies.

  For more information, see Password policies for SAP user accounts on page 112.

- Initial password for new user accounts

  You have the different options for issuing an initial password for user accounts. Enter a password or use a random generated initial password when you create a user account.

  For more information, see Initial password for new SAP user accounts on page 123.
- Email notifications about credentials

  When a new user account is created, the login data are sent 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 credentials on page 123.
- Login languages

  User accounts can be assigned a default login language. Login languages can be loaded in to the One Identity Manager database through synchronization.

  For more information, see Login languages on page 109.
- Target system types

  Target system types are required for configuring target system comparisons. Tables with outstanding objects are maintained with the target system types and settings are configured for provisioning memberships and single objects synchronization. Target system types also map objects in the Unified Namespace.

  For more information, see Post-processing outstanding objects on page 58.
- Servers

  In order to handle target system specific processes in One Identity Manager, the synchronization server and its server functionality must be declared.

  For more information, see Editing a server on page 90.
- Target system managers

  A default application role exists for the target system manager in One Identity Manager. Assign identities to this application role who have permission to edit all clients in One Identity Manager.

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

  For more information, see Target system managers on page 96.

Setting up account definitions

One Identity Manager has account definitions for automatically allocating user accounts to identities. You can create account definitions for every target system. If an identity 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 identity.

The data for the user accounts in the respective target system comes from the basic identity main data. The identities must have a central an SAP user account. The assignment of the IT operating data to the identity's user account is controlled through the primary assignment of the identity to a location, a department, a cost center, or a business role. 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 more 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 formatting rule for IT operating data
- Collecting IT operating data
- Assigning account definitions to identities
- Assigning account definitions to a target system

In SAP R/3, if user accounts are managed 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 136.

Creating an account definition

To create or edit an account definition

1. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list. Select the **Change main data** task.

   -OR-

   Click in the result list.
3. Enter the account definition's main data.
4. Save the changes.

Detailed information about this topic

- Main data for an account definition on page 73

Main data for an account definition

Enter the following data for an account definition:

Table 22: Main data for an account definition

Property	Description
Account definition	Account definition name.
User account table	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 clients of central user administration (CUA) system, select **SAPUserMandant**.
Target system	Target system to which the account definition applies.
Required account definition	Specifies the required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is assigned automatically. If you want the account definition to provide access to clients 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 identity does not yet have a user account. For an account definition to create user accounts, leave this field empty.
Description	Text field for additional explanation.
Manage level (initial)	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.
Risk index	Value for evaluating the risk of assigning the account definition to identities. Set a value in the range **0** to **1**. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Service item	Service item through which you can request the account definition resource in the IT Shop. Assign an existing service item or add a new one.

Property	Description
IT Shop	Specifies whether the account definition can be requested through the IT Shop. This account definition can be requested through the Web Portal and allocated by defined approval processes. The resource can also be assigned directly to identities and roles outside the IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. This account definition can be requested through the Web Portal and allocated by defined approval processes. The account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to identities	Specifies whether the account definition is automatically assigned to all internal identities. To automatically assign the account definition to all internal identity, use the **Enable automatic assignment to identities** The account definition is assigned to every identity that is not marked as external. Once a new internal identity is created, they automatically obtain this account definition. To automatically remove the account definition assignment from all identities, use the **Disable automatic assignment to identities**. The account definition cannot be reassigned to identities from this point on. Existing account definition assignments remain intact.
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently deactivated identities. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition if temporarily disabled	Specifies the account definition assignment to temporarily deactivated identities. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition on deferred deletion	Specifies the account definition assignment on deferred deletion of identities. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.

Property	Description
Retain account definition on security risk	Specifies the account definition assignment to identities posing a security risk. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.
Groups can be inherited	Specifies whether the user account can inherit groups through the linked identity. If the option is set, the user account inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests. • If you add an identity 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 identity has requested group membership in the IT Shop and the request is granted approval, the identity's user account only inherits the group if the option is set.
Roles can be inherited	Specifies whether the user account can inherit SAP roles through the linked identity. If the option is set, the user account inherits the roles through hierarchical roles, in which the identity is a member, or through IT Shop requests.
Profiles can be inherited	Specifies whether the user account can inherit profiles through the linked identity. If the option is set, the user account inherits profiles through hierarchical roles, in which the identity is a member, or through IT Shop requests.

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 identity’s properties that are inherited by the user account. This allows an identity to have several user accounts in one target system, for example:

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

One Identity Manager supplies a default configuration for manage levels:

- **Unmanaged**: User accounts with the **Unmanaged** manage level are linked to the identity but they do no inherit any further properties. When a new user account is added with this manage level and an identity is assigned, some of the identity's properties are transferred initially. If the identity 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 identity. When a new user account is created with this manage level and an identity is assigned, the identity's properties are transferred in an initial state. If the identity properties are changed at a later date, the changes are passed onto the user account.

NOTE: The **Full managed** and **Unmanaged** manage levels 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 how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships at each manage level. For more information about manage levels, see the *One Identity Manager Target System Base Module Administration Guide*.

- Identity user accounts can be locked when they are disabled, deleted, or rated as a security risk so that permissions are immediately withdrawn. If the identity is reinstated at a later date, the user accounts are also reactivated.
- You can also define group membership inheritance. Inheritance can be discontinued if desired when, for example, the identity’s user accounts are disabled and therefore cannot be members in groups. During this time, no inheritance processes should be calculated for this identity. Existing group memberships are deleted.

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

To assign manage levels to an account definition

1. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign manage level** task.
4. In the **Add assignments** pane, assign the manage level.

   TIP: In the **Remove assignments** pane, you can remove assigned manage levels.

To remove an assignment

- Select the manage level and double-click .

5. Save the changes.

To edit a manage level

1. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Manage levels** category.
2. Select the manage level in the result list. Select **Change main data**.

   - OR -

   Click in the result list.
3. Edit the manage level's main data.
4. Save the changes.

Detailed information about this topic

- Main data for manage levels on page 77

Main data for manage levels

Enter the following data for a manage level.

Table 23: Main data for manage levels

Property	Description
Manage level	Name of the manage level.
Description	Text field for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: • **`Never`**: Data is not updated. (Default) • **`Always`**: Data is always updated. • **`Only initially`**: Data is only determined at the start.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily deactivated retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily deactivated identities are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently deactivated identities retain group memberships.
Lock user accounts if	Specifies whether user accounts of permanently deactivated

Property	Description
permanently disabled	identities are locked.
Retain groups on deferred deletion	Specifies whether user accounts of identities marked for deletion retain their group memberships.
Lock user accounts if deletion is deferred	Specifies whether user accounts of identities marked for deletion are locked.
Retain groups on security risk	Specifies whether user accounts of identities posing a security risk retain their group memberships.
Lock user accounts if security is at risk	Specifies whether user accounts of identities posing a security risk are locked.
Retain groups if user account disabled	Specifies whether disabled user accounts retain their group memberships.

Creating a formatting 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 identity's primary roles.

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

- Groups can be inherited
- Roles can be inherited
- Profiles can be inherited
- Identity
- Privileged user account.

To create a mapping rule for IT operating data

1. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Edit IT operating data mapping** task.
4. Click **Add** and enter the following information:
    - **Column**: User account property for which the value is set. In the drop-down, you can select the columns that use the `TSB_ITDataFromOrg` script in their

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

- **Source**: Specifies which roles to use in order to find the user account properties. You have the following options:
  - Primary department
  - Primary location
  - Primary cost center
  - Primary business roles

    NOTE: The business role can only be used if the Business Roles Module is available.
  - Empty

    If you select a role, you must specify a default value and set the **Always use default value** option.
- **Default value**: Default value of the property for an identity's user account if the value is not determined dynamically from the IT operating data.
- **Always use default value**: Specifies whether the user account property is always set with the default value. IT operating data is not determined dynamically from a role.
- **Notify when applying the default**: Specifies whether an email is sent to a specific mailbox when the default value is used. The **Identity - new user account with default properties created** mail template is used.

  To change the mail template, in the Designer, adjust the **TargetSystem | SAPR3 | Accounts | MailTemplateDefaultValues** configuration parameter.

5. Save the changes.

Collecting IT operating data

To create user accounts for an identity with the **Full managed** manage level, you need to know which IT operating data is required. The operating data required for each specific target system is defined with its business roles, departments, locations, or cost centers. An identity 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: Mapping IT operating data

Normally, each identity in department A obtains a default user account in the tenant A. In addition, certain identities in department A obtain administrative user accounts in the tenant 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.In the IT operating data mapping rule for the account definitions A and B, specify the `Department` property 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, for department A, specify the effective IT operating data of account definition B. This IT operating data is used for administrative user accounts.

To define IT operating data

1. In the 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.
    - **Effects on**: Specify an 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

      a. Click → next to the field.

      b. Under **Table**, select the table that maps the target system for select the `TSBAccountDef` table or an account definition.

      c. Select the specific target system or account definition under **Effects on**.

      d. Click **OK**.
    - **Column**: Select the user account property for which the value is set.

      In the drop-down, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.
    - **Value**: Enter a fixed value to assign to the user account's property.
4. Save the changes.

Modify IT operating data

If IT operating data changes, you must transfer the 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, a cost center, a business role, or a location have been changed.

  - OR -

- The default values in the IT operating data template were modified for an account definition.

NOTE: If the assignment of an identity to a primary department, cost center, to a primary business role or to a primary location changes, the templates are automatically run.

To run the template

1. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Run templates** task.

   This displays a list of all user accounts that were created with the selected account definition and whose properties were changed by modifying the IT operating data. That means:

   - **Old value**: Value of the object property before changing the IT operating data.
   - **New value**: Value of the object property after changing the IT operating data.
   - **Selection**: Specifies whether the new value is copied to 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 identities

Account definitions are assigned to company identities.

Indirect assignment is the default method for assigning account definitions to identities. Account definitions are assigned to departments, cost centers, locations, or roles. The identities 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 identities.

You can automatically assign special account definitions to all company identities. It is possible to assign account definitions to the IT Shop as requestable products. Department

managers can then request user accounts from the Web Portal for their staff. It is also possible to add account definitions to system roles. These system roles can be assigned to identities through hierarchical roles or added directly to the IT Shop as products.

In the One Identity Manager default installation, the processes are checked at the start to see if the identity 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. In this case, you must change the user account manage level afterward.

As long as an account definition for an identity is valid, the identity retains the user account that was created by it. If the account definition assignment is removed, the user account that was created from this account definition, is deleted. User accounts marked as **Outstanding** are only deleted if the **QER | Person | User | DeleteOptions | DeleteOutstanding** configuration parameter is set.

Prerequisites for indirect assignment of account definitions to identities

- Assignment of identities and account definitions is permitted for role classes (departments, cost centers, locations, or business roles).

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.

   - OR -

   In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.
2. Select the **Configure role assignments** task and configure the permitted assignments.
   - To generally allow an assignment, enable the **Assignments allowed** column.
   - To allow direct assignment, enable the **Direct assignments permitted** column.
3. Save the changes.

For more 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 83
- Assigning account definitions to business roles on page 83
- Assigning account definitions to all identities on page 84
- Assigning account definitions directly to identities on page 84
- Assigning account definitions to a target system on page 88

Assigning account definitions to departments, cost centers, and locations

Assign account definitions to departments, cost centers, and locations in order to assign identities to them through these organizations.

To add account definitions to hierarchical roles

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

    TIP: In the **Remove assignments** pane, you can remove assigned organizations.

    To remove an assignment

    - Select the organization and double-click ✓.
5. Save the changes.

Assigning account definitions to business roles

NOTE: This function is only available if the Business Roles Module is installed.

You can assign account definitions to business roles in order to assign them to identities through business roles.

To add account definitions to hierarchical roles

1. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, select the role class and assign business roles.

    TIP: In the **Remove assignments** pane, you can remove assigned business roles.

    To remove an assignment

    - Select the business role and double-click ✓.
5. Save the changes.

Assigning account definitions to all identities

Use this task to assign the account definition to all internal identities. Identities that are marked as external do not obtain this account definition. Once a new internal identity is created, they automatically obtain this account definition. The assignment is calculated by the DBQueue Processor.

IMPORTANT: Only run this task if you can ensure that all current internal identities in the database and all pending newly added internal identities obtain a user account in this target system.

To assign an account definition to all identities

1. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Change main data** task.
4. Select the **Disable automatic assignment to identities** task.
5. Confirm the security prompt with **Yes**.
6. Save the changes.

NOTE: To automatically remove the account definition assignment from all identities, run the DISABLE AUTOMATIC ASSIGNMENT TO IDENTITIES task. The account definition cannot be reassigned to identities from this point on. Existing assignments remain intact.

Assigning account definitions directly to identities

Account definitions can be assigned directly or indirectly to identities. Indirect assignment is carried out by allocating identities and account definitions in company structures, like departments, cost centers, locations, or business roles.

To react quickly to special requests, you can assign account definitions directly to identities.

To assign an account definition directly to identities

1. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign to identities** task.
4. In the **Add assignments** pane, add identities.

   TIP: In the **Remove assignments** pane, you can remove assigned identities.

To remove an assignment

- Select the identity and double-click ✓.

5. Save the changes.

Assigning account definitions to system roles

NOTE: This function is only available if the System Roles Module is installed.

Use this task to add an account definition to system roles.

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

To add account definitions to a system role

1. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

   TIP: In the **Remove assignments** pane, you can remove the system role assignment.

   To remove an assignment

   - Select the system role and double-click ✓.

5. Save the changes.

Adding account definitions to the IT Shop

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

- If the account definition is only assigned to identities using IT Shop assignments, you must also set the **Only for use in IT Shop** option. 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 (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. To assign the account definition to shelves, select the **IT Shop shelves** tab and, in the **Add assignments** section, select the shelves with a double-click.
5. To assign the account definition to IT Shop templates, select the **IT Shop templates** tab and, in the **Add assignments** section, select the template with a double-click.
6. Save the changes.

To add an account definition to the IT Shop (non role-based login)

1. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. To assign the account definition to shelves, select the **IT Shop shelves** tab and, in the **Add assignments** section, select the shelves with a double-click.
5. To assign the account definition to IT Shop templates, select the **IT Shop templates** tab and, in the **Add assignments** section, select the template with a double-click.
6. Save the changes.

To remove an account definition from individual IT Shop shelves (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. To remove the account definition from the shelves, select the **IT Shop shelves** tab and, in the **Remove assignments** section, double-click the shelves.
5. To remove the account definition from the IT Shop templates, select the **IT Shop templates** tab and, in the **Remove assignments** section, double-click the templates.
6. Save the changes.

To remove an account definition from individual IT Shop shelves (non role-based login)

1. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.

4. To remove the account definition from the shelves, select the **IT Shop shelves** tab and, in the **Remove assignments** section, double-click the shelves.
5. To remove the account definition from the IT Shop templates, select the **IT Shop templates** tab and, in the **Remove assignments** section, double-click the templates.
6. Save the changes.

To remove an account definition from all IT Shop shelves (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

   The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

To remove an account definition from all IT Shop shelves (non role-based login)

1. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

   The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

For more information about requesting company resources through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Related topics

- Main data for an account definition on page 73
- Assigning account definitions to departments, cost centers, and locations on page 83
- Assigning account definitions to business roles on page 83
- Assigning account definitions directly to identities on page 84
- Assigning account definitions to system roles on page 85

Assigning account definitions to a target system

NOTE: To use automatic identity assignment for central user administration (CUA) user accounts, assign an 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 identities resulting in administered user accounts (**Linked configured** state):

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

User accounts are only linked to the identity (**Linked** state) 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 the Manager, select the client in the **SAP R/3 > Clients** category.
2. Select the **Change main data** task.
3. From the **Account definition (initial)** drop-down, select the account definition for user accounts.
4. Save the changes.

Deleting an account definition

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

To delete an account definition

1. Remove automatic assignments of the account definition from all identities.
    a. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.
    b. Select an account definition in the result list.
    c. Select the **Change main data** task.
    d. Select the **Disable automatic assignment to identities** task.
    e. Confirm the security prompt with **Yes**.
    f. Save the changes.
2. Remove direct assignments of the account definition to identities.

a. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Assign to identities** task.

d. In the **Remove assignments** pane, remove identities.

e. Save the changes.

3. Remove the account definition's assignments to departments, cost centers, and locations.

a. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Assign organizations** task.

d. In the **Remove assignments** pane, remove the relevant departments, cost centers, and locations.

e. Save the changes.

4. Remove the account definition's assignments to business roles.

a. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Assign business roles** task.

d. In the **Remove assignments** pane, remove the business roles.

e. 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 information about unsubscribing requests, see the *One Identity Manager Web Portal User Guide*.

   To remove an account definition from all IT Shop shelves (role-based login)

   a. In the Manager, select the **Entitlements > Account definitions** category.

   b. Select an account definition in the result list.

   c. Select the **Remove from all shelves (IT Shop)** task.

   d. Confirm the security prompt with **Yes**.

   e. Click **OK**.

      The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

To remove an account definition from all IT Shop shelves (non role-based login)

a. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Remove from all shelves (IT Shop)** task.

d. Confirm the security prompt with **Yes**.

e. Click **OK**.

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

6. Remove the required account definition assignment. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.

a. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Change main data** task.

d. From the **Required account definition** drop-down, remove the account definition.

e. Save the changes.

7. Remove the account definition's assignments to target systems.

a. In the Manager, select the client in the **SAP R/3 > Clients** category.

b. Select the **Change main data** task.

c. On the **General** tab, remove the assigned account definitions.

d. Save the changes.

8. Delete the account definition.

a. In the Manager, select the **SAP R/3 > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Click to delete an account definition.

Editing a server

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

- In the Designer, create an entry for the Job server in the **Base Data > Installation > Job server** category. For more information about this, see the *One Identity Manager Configuration Guide*.
- Select an entry for the Job server in **Manager > Basic configuration data > Server** in SAP R/3 and edit the Job server main 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 perform 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 the Manager, select the **SAP R/3 > Basic configuration data > Server** category.
2. Select the Job server entry in the result list.
3. Select the **Change main data** task.
4. Edit the Job server's main data.
5. Select the **Assign server functions** task and specify server functionality.
6. Save the changes.

Detailed information about this topic

- Main data for a Job server on page 91
- Specifying server functions on page 94

Related topics

- Setting up the synchronization server on page 21

Main data for a Job server

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

The following properties are displayed for Job servers.

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

Table 24: Job server properties

Property	Meaning
Server	Job server name.

Property	Meaning
Full server name	Full server name in accordance with DNS syntax. Syntax: `<Name of servers>.<Fully qualified domain name>`
Target system	Computer account target system.
Language	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The **Server is cluster** and **Server belongs to cluster** properties are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Copy process (source server)	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. 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.
Copy process (target server)	Permitted copying methods that can be used when this server is the destination of a copy action.
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.
Executing server	Name of the executing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the

Property	Meaning
	process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. The process steps are requested by the Job queue using this queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values **Win32**, **Windows**, **Linux**, and **Unix** are permitted. If no value is specified, **Win32** is used.
Service account data	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.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure 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.
Stop One Identity Manager Service	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 Job Queue Info program. For more information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.
Paused due to unavailability of a target system	Specifies whether task processing for this queue has been stopped because the target system that uses this Job server as a synchronization server is temporarily unavailable. As soon as the target system is available again, processing starts and all outstanding tasks are performed.

Property	Meaning
	For more information about offline mode, see the *One Identity Manager Target System Synchronization Reference Guide*.
No automatic software update	Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently running.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

Related topics

- Specifying server functions on page 94

Specifying server functions

NOTE: All editing options are also available in the 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 with respect to the server function.

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

Table 25: Permitted server functions

Server function	Remark
CSV connector	Server on which the CSV connector for synchronization is installed.
Domain controller	The Active Directory domain controller. Servers that are not labeled as domain controllers are considered to be member servers.
Printer server	Server that acts as a print server.
Generic server	Server for generic synchronization with a custom target system.
Home server	Server for adding home directories for user accounts.
Update server	This server automatically updates the software on all

Server function	Remark
	the other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. It can run SQL tasks. The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.
SQL processing server	It can run SQL tasks. The server requires a direct connection to the database server that One Identity Manager database is installed on. 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.
CSV script server	This server can process CSV files using the `ScriptComponent` process component.
Generic database connector	This server can connect to an ADO.Net database.
One Identity Manager database connector	Server on which the One Identity Manager connector is installed. This server synchronizes the One Identity Manager target system.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
Primary domain controller	Primary domain controller.
Profile server	Server for setting up profile directories for user accounts.
SAM synchronization Server	Server for synchronizing an SMB-based target system.
SAP R/3 connector	Server on which the SAP R/3 connector is installed. This server synchronizes the SAP R/3 target system.
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
PowerShell connector	The server can run PowerShell.

Related topics

- Main data for a Job server on page 91

Target system managers

A default application role exists for the target system manager in One Identity Manager. Assign identities to this application role who have permission to edit all clients in One Identity Manager.

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

For more 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 allocates identities to be target system administrators.
2. These target system administrators add identities to the default application role for target system managers.

   Target system managers with the default application role are authorized to edit all the clients in One Identity Manager.
3. Target system managers can authorize other identities within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual clients.

   NOTE: If no identities are assigned to a child application role for target system administrators, the identities of the parent application role are granted the permissions.

Table 26: Default application roles for target system managers

User	Tasks
Target system managers	Target system managers must be assigned to the **Target systems | SAP R/3** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects. • Edit password policies for the target system. • Prepare system entitlements to add to the IT Shop. • Can add identities that do not have the **Primary identity** identity type. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.

User	Tasks
	• Edit the synchronization's target system types and outstanding objects. • Authorize other identities within their area of responsibility as target system managers and create child application roles if required.

To initially specify identities to be target system administrators

1. Log in to the Manager as a One Identity Manager administrator (**Base role | Administrators** application role)
2. Select the **One Identity Manager Administration > Target systems > Administrators** category.
3. Select the **Assign identities** task.
4. Assign the identity and save the changes.

To add the first identities to the default application as target system managers

1. Log in to the Manager as a target system administrator (**Target systems | Administrators** application role).
2. Select the **One Identity Manager Administration > Target systems > SAP R/3** category.
3. Select the **Assign identities** task.
4. Assign the identities you want and save the changes.

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

1. Log in to the Manager as a target system manager.
2. Select the application role in the **SAP R/3 > Basic configuration data > Target system managers** category.
3. Select the **Assign identities** task.
4. Assign the identities you want and save the changes.

To specify target system managers for individual clients

1. Log in to the Manager as a target system manager.
2. Select the **SAP R/3 > Clients** category.
3. Select the client in the result list.
4. Select the **Change main data** task.
5. On the **General** tab, select the application role in the **Target system manager** drop-down.

   - OR -

Next to the **Target system manager** drop-down, 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 identities to this application role who are permitted to edit the client in One Identity Manager.

Related topics

- One Identity Manager users for managing SAP R/3 on page 12
- General main data of SAP clients on page 127

4

Basic data for user account administration

One Identity Manager supplies the following basic data for user administration, by default:

- User account types on page 99
- External identifier types on page 100

If configured, other basic data that cannot be edited in One Identity Manager is read from SAP R/3 during synchronization. It is used only for assignments to SAP user accounts. These include:

- SAP parameters on page 101
- Printers on page 108
- Cost centers on page 109
- Start menus on page 109
- Companies on page 109
- Login languages on page 109
- Licenses on page 110
- Special versions on page 111

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 123
- Email notifications about login credentials on page 123

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 27: User account types

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

The default user account type for new user accounts is specified in the "TargetSystem | SAPR3 | Accounts | Ustyp" configuration parameter.

To modify the default user account type

- In the Designer, edit the value of the "TargetSystem | SAPR3 | Accounts | Ustyp" configuration parameter.

External identifier types

External authentication methods for logging in 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 28: External identifier types

Type	Description
DN	Distinguished Name for X.509.
NT	Windows NTLM or password verification with the Windows domain controller.
LD	LDAP bind <user-defined> (For other external authentication mechanisms).
SA	SAML Token.

To specify a default type for external identifiers

- In the Designer, set the "TargetSystem | SAPR3 | UserDefaults | ExtID_Type" configuration parameter and specify a value.

SAP parameters

Parameters can be loaded into the One Identity Manager database by synchronization and be either directly or indirectly assigned to user accounts. In the case of indirect assignment, identities and parameters are arranged in hierarchical roles. The number of parameters assigned to an identity is calculated from the position in the hierarchy and the direction of inheritance. If you add an identity to hierarchical roles and that identity owns a user account, the parameter is assigned to the user account.

Prerequisites for assigning identities to user accounts are:

- Assignment of identities and SAP parameters is permitted for role classes (departments, cost centers, locations, or business roles).
- User accounts and parameters belong to the same SAP system.

A different parameter value can be specified for each hierarchical role that is assigned a parameter. Thus, the parameter values are also inherited by the user account. You can use membership in hierarchical roles to control which parameter values the parameter obtain from the user account.

Parameters can also be added to SAP products or other system roles and assigned to user accounts through these.

Detailed information about this topic

- Displaying main data of SAP parameters on page 101
- General main data of SAP parameters on page 102
- Assigning SAP parameters to departments, cost centers, and locations on page 102
- Assigning SAP parameters to business roles on page 103
- Assigning SAP parameters to system roles on page 104
- Editing parameter values for indirect SAP parameter assignment on page 105
- Inheritance of parameter values by SAP user accounts on page 107

Related topics

- Directly assigning SAP parameters on page 150
- SAP products on page 202

Displaying main data of SAP parameters

To display the properties of a parameter

1. In the Manager, select the **SAP R/3 > Parameters** category.
2. Select the parameter in the result list.

3. Select the **Change main data** task.

To obtain an overview of a parameter

1. In the Manager, select the **SAP R/3 > Parameters** category.
2. Select the parameter in the result list.
3. Select the **Parameter overview** task.

On the parameter's overview form, you can click the assigned user account to open the user account's main data form. You can adjust the values of the parameters that modify this assignment.

Detailed information about this topic

- Directly assigning SAP parameters on page 150

General main data of SAP parameters

The following properties are mapped for parameters

Table 29: Parameter properties

Property	Description
System	System to which the parameter belongs.
Parameter	Parameter name.
Text	Description of the parameter.

Assigning SAP parameters to departments, cost centers, and locations

Assign parameters to departments, cost centers, and locations so that they are assigned to user accounts through these organizations.

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

1. In the Manager, select the **SAP R/3 > Parameters** category.
2. Select the parameter in the result list.
3. Select the **Assign organizations** task.

4. In the **Add assignments** pane, assign the organizations:
    - On the **Departments** tab, assign departments.
    - On the **Locations** tab, assign locations.
    - On the **Cost centers** tab, assign cost centers.

    TIP: In the **Remove assignments** pane, you can remove assigned organizations.

    To remove an assignment
    - Select the organization and double-click ✓.
5. Save the changes.

To assign parameters to a department, cost center, or location (role-based login)

1. In the Manager, select the **Organizations > Departments** category.

    - OR -

    In the Manager, select the **Organizations > Cost centers** category.

    - OR -

    In the Manager, select the **Organizations > Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign SAP parameters** task.
4. In the **Add assignments** pane, assign parameters. To filter the parameter list, select a system in the **SAP systems** field.

    TIP: In the **Remove assignments** pane, you can remove parameter assignments.

    To remove an assignment
    - Select the parameter and double-click ✓.
5. Save the changes.

Related topics

- Assigning SAP parameters to business roles on page 103
- Editing parameter values for indirect SAP parameter assignment on page 105
- Directly assigning SAP parameters on page 150
- One Identity Manager users for managing SAP R/3 on page 12

Assigning SAP parameters to business roles

NOTE: This function is only available if the Business Roles Module is installed.

By assigning a parameter to business roles, you are assigning the parameter to user accounts through these business roles.

To assign a parameter to business roles (non role-based login)

1. In the Manager, select the **SAP R/3 > Parameters** category.
2. Select the parameter in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, select the role class and assign business roles.

   TIP: In the **Remove assignments** pane, you can remove assigned business roles.

   To remove an assignment

   - Select the business role and double-click ✓.
5. Save the changes.

To assign parameters to a business role (non role-based login)

1. In the Manager, select the **Business roles > <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign SAP parameters** task.
4. In the **Add assignments** pane, assign parameters. To filter the parameter list, select a system in the **SAP systems** field.

   TIP: In the **Remove assignments** pane, you can remove parameter assignments.

   To remove an assignment

   - Select the parameter and double-click ✓.
5. Save the changes.

Related topics

- Assigning SAP parameters to departments, cost centers, and locations on page 102
- Editing parameter values for indirect SAP parameter assignment on page 105
- Directly assigning SAP parameters on page 150
- One Identity Manager users for managing SAP R/3 on page 12

Assigning SAP parameters to system roles

Installed modules: System Roles Module

SAP parameters can be added to different system roles. If you assign a system role to identities, all SAP user accounts owned by these identities inherit the parameters. Parameters can also be added to system roles that are not SAP products.

To assign a parameter to system roles

1. Select the **SAP R/3 > Parameters** category.
2. Select the parameter in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

   TIP: In the **Remove assignments** pane, you can remove the system role assignment.

   To remove an assignment

   - Select the system role and double-click ✓.
5. Save the changes.

Detailed information about this topic

- SAP products on page 202

Related topics

- Assigning SAP parameters to departments, cost centers, and locations on page 102
- Assigning SAP parameters to business roles on page 103
- Directly assigning SAP parameters on page 150
- Assigning SAP parameter to SAP products on page 211
- Editing parameter values for indirect SAP parameter assignment on page 105

Editing parameter values for indirect SAP parameter assignment

To add, change or delete a parameter value for indirect parameter assignment

1. In the Manager, select the **Organizations > Departments** category.
2. In the result list, select the department the parameter is assigned to.
3. Select the **Department overview** task.
4. In the **SAP parameter** form element, select a parameter.

   This opens the parameter assignment main data form.
5. Add, edit, or delete the parameter value.
6. Save the changes.

- OR -

1. In the Manager, select the **Organizations > Cost centers** category.
2. In the result list, select the cost center the parameter is assigned to.
3. Select the **Cost center overview** task.
4. In the **SAP parameter** form element, select a parameter.
   This opens the parameter assignment main data form.
5. Add, edit, or delete the parameter value.
6. Save the changes.

- OR -

1. In the Manager, select the **Organizations > Locations** category.
2. In the result list, select the location the parameter is assigned to.
3. Select the **Location overview** task.
4. In the **SAP parameter** form element, select a parameter.
   This opens the parameter assignment main data form.
5. Add, edit, or delete the parameter value.
6. Save the changes.

- OR -

1. In the Manager, select the **Business roles > <role class>** category.
2. In the result list, select the business role the parameter is assigned to.
3. Select the **Business role overview** task.
4. In the **SAP parameter** form element, select a parameter.
   This opens the parameter assignment main data form.
5. Add, edit, or delete the parameter value.
6. Save the changes.

- OR -

1. In the Manager, select the **SAP R/3 > Products** category.
   - OR -
   In the Manager, select the **Entitlements > System roles** category.
2. In the result list, select the system role the parameter is assigned to.
3. Select the **Assign SAP parameters** task.
4. In the **Remove assignments** pane, select the assigned parameters.
5. Select the **Extended properties** context menu.
   This opens the parameter assignment main data form.
6. Add, edit, or delete the parameter value.
7. Save the changes.

Related topics

- Assigning SAP parameters to departments, cost centers, and locations on page 102
- Assigning SAP parameters to business roles on page 103
- Assigning SAP parameters to system roles on page 104
- Directly assigning SAP parameters on page 150
- Inheritance of parameter values by SAP user accounts on page 107

Inheritance of parameter values by SAP user accounts

If parameters are directly assigned to user accounts, you can enter a parameter value. You can also specify a parameter value if parameters are assigned to hierarchical roles or system roles. This parameter value is inherited by the user account along with the parameter. If a parameter is inherited by a user account by different methods, the actual parameter value is calculated as followed:

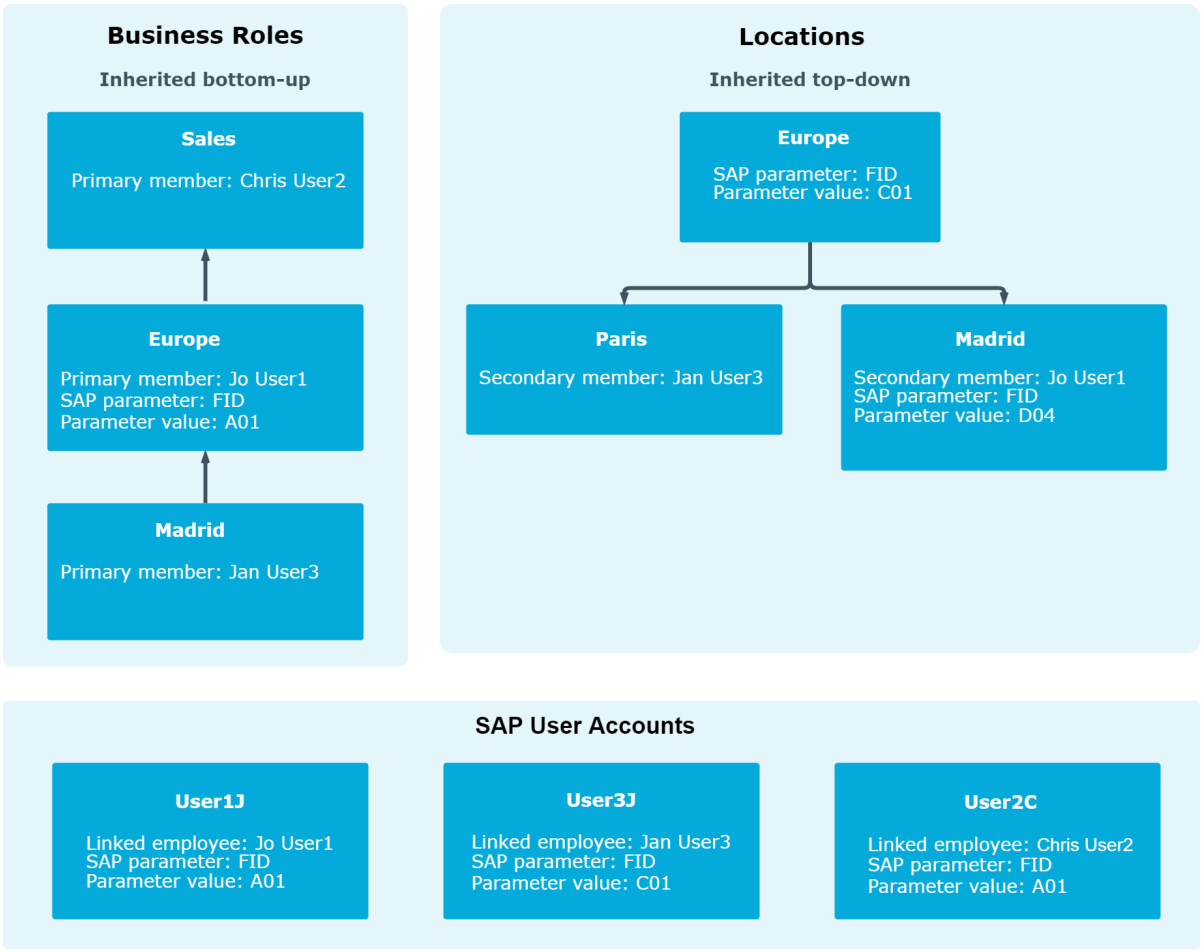
1. Directly assigned parameters are determined.

   Direct assignments come about by:

   - Synchronizing user accounts including their parameter values
   - Direct assignment of parameters in the Manager

2. Indirectly assigned parameter are determined in the following order:
   a. System role
   b. Primary department
   c. Primary location
   d. Primary cost center
   e. Primary business roles
   f. Secondary department
   g. Secondary location
   h. Secondary cost center
   i. Secondary business role
3. If the parameter is inherited through different roles of a role class, the actual parameter value is calculated by the shortest inheritance path within the role hierarchy. The direction of inheritance of the role class is taken into account.
4. If a parameter with various values is inherited from a role class through different roles and the inheritance path in the role hierarchy is the same length, then the smallest value is found.

Figure 4: Example of SAP parameter inheritance



Related topics

- Editing parameter values for indirect SAP parameter assignment on page 105
- Directly assigning SAP parameters on page 150

Printers

To display a printer

1. Select the **SAP R/3 > Printers** category.
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 the **SAP R/3 > Start menus** category.
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 the **SAP R/3 > Companies** category.
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 the **SAP R/3 > Basic configuration data > Login languages** category.
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 the **SAP R/3 > Security policies** category.
2. Select the security policy in the result list. Select the **Change main data** task.

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 the **SAP R/3 > Communication types** category.
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 the **SAP R/3 > Licenses** category.
2. Select the license in the result list. Select the **Change main data** task.
3. Enter a value in **Rating**.
4. Save the changes.

The following information is shown for Licenses:

Table 30: License main data

Property	Description
License	Unique license identifier. Used to determine the system measurement rating if no license rating is entered.
system	Associated SAP system.
User type	User type of the SAP system to which the license applies.
Price list (token)	Number in the price list.
Price list (text)	Description in the price list.
Rating	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 determined. If no rating is entered the license ID for determining the rating for system measurement is used.
Enabled	Specifies whether the license is enabled.
Special version	Specifies whether special versions can be selected for this license.
Country surcharge	Specifies whether country surcharges can be selected for this license.

Detailed information about this topic

- Providing system measurement data on page 215

Special versions

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

You can display 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 a special version

1. Select the **SAP R/3 > Special versions** category.
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 identities' 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 use or customize if required. You can also define your own password policies.

Detailed information about this topic

- Predefined password policies on page 112
- Using password policies on page 113
- Editing password policies on page 115
- Custom scripts for password requirements on page 119
- Password exclusion list on page 121
- Checking a password on page 122
- Testing password generation on page 122

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 defines the settings for the system user passwords (`DialogUser.Password` and `Person.DialogUserPassword`) as well as the passcode for a one time 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 identities, user accounts, or system users.

For more information about password policies for identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policy for forming identities' central passwords

An identity's central password is formed from the target system specific user accounts by respective configuration. The **Identity central password policy** defines the settings for

the (`Person.CentralPassword`) central password. Members of the **Identity Management | Identities | Administrators** application role can adjust this password policy.

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

For more information about password policies for identities, 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** default policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

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 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.

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

1. Password policy of the user account's account definition.
2. Password policy of the user account's manage level.
3. Password policy of the user account's client.
4. The **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** default 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.
    - **Apply to**: Application scope of the password policy.

      To specify an application scope

      1. Click → next to the field.
      2. Select one of the following references under **Table**:
          - The table that contains the base objects of synchronization.
          - To apply the password policy based on the account definition, select the `TSBAccountDef` table.
          - To apply the password policy based on the manage level, select the `TSBBehavior` table.
      3. Under **Apply to**, select the table that contains the base objects.
          - If you have selected the table containing the base objects of synchronization, next select the specific target system.
          - If you have selected the `TSBAccountDef` table, next select the specific account definition.
          - If you have selected the `TSBBehavior` table, next select the specific manage level.
      4. Click **OK**.
    - **Password column**: Name of the password column.
    - **Password policy**: Name of the password policy to use.
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 the **Assign objects** task.
4. In the **Assignments** pane, select the assignment you want to change.
5. From the **Password Policies** drop-down, select the new password policy you want to apply.
6. Save the changes.

Editing password policies

Predefined password policies are supplied with the default installation that you can use or customize if required.

To edit a password policy

1. In the Manager, select the **SAP R/3 > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Edit the password policy's main data.
5. Save the changes.

Detailed information about this topic

- General main data of password policies on page 115
- Policy settings on page 116
- Character classes for passwords on page 117
- Custom scripts for password requirements on page 119

General main data of password policies

Enter the following main data of a password policy.

Table 31: main data for a password policy

Property	Meaning
Display name	Password policy name. Translate the given text using the button.
Description	Text field for additional explanation. Translate the given text using the button.
Error Message	Custom error message generated if the policy is not fulfilled. Translate the given text using the button.
Owner (Application Role)	Application roles whose members can configure the password policies.
Default policy	Mark as default policy for passwords. This option cannot be changed. NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is

Property	Meaning
	applied if no other password policy can be found for identities, user accounts, or system users.

Policy settings

Define the following settings for a password policy.

Table 32: Policy settings

Property	Meaning
Initial password	Initial password for newly created user accounts. The initial password is used if a password is not entered when you create a user account or if a random password is not generated.
Password confirmation	Reconfirm password.
Minimum Length	Minimum length of the password. Specify the number of characters a password must have. If the value is **0**, no password is required.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is **256**.
Max. errors	Maximum number of errors. Set the number of invalid passwords attempts. The number of failed logins is only taken into account when logging in to One Identity Manager. If the value is **0**, the number of failed logins is not taken into account. This data is only taken into account if the One Identity Manager login was through a system user or identity based authentication module. If a user has exceeded the maximum number of failed logins, the identity or system user will not be able to log in to One Identity Manager. You can use the Password Reset Portal to reset the passwords of identities and system users who have been locked. For more information, see the *One Identity Manager Web Portal User Guide*.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires. If the value is **0**, then the password does not expire.
Password history	Enter the number of passwords to be saved. If, for example, a value of **5** is entered, the user's last five passwords are

Property	Meaning
	stored. If the value is **0**, then no passwords are stored in the password history.
Minimum password strength	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.
Name properties denied	Specifies whether name properties are permitted in the password. If this option is set, name properties are not permitted in passwords. The values of these columns are taken into account if the **Contains name properties for password check** option is set. In the Designer, adjust this option in the column definition. For more information, see the *One Identity Manager Configuration Guide*.

Character classes for passwords

Specify which characters are permitted for a password.

Table 33: Character classes for passwords

Property	Meaning
Required number of character classes	Number of rules for character classes that must be fulfilled so that a password adheres to the password policy. The following rules are taken into account for **Min. number letters**, **Min. number lowercase**, **Min. number uppercase**, **Min. number digits**, and **Min. number special characters**. That means: • Value **0**: All character class rules must be fulfilled. • Value **>0**: Minimum number of character class rules that must be fulfilled. At most, the value can be the number of rules with a value **>0**. NOTE: Generated passwords are not tested for this.
Min. number letters	Specifies the minimum number of alphabetical characters the password must contain.
Min. number lowercase	Specifies the minimum number of lowercase letters the password must contain.

Property	Meaning
Min. number uppercase	Specifies the minimum number of uppercase letters the password must contain.
Min. number digits	Specifies the minimum number of digits the password must contain.
Min. number special characters	Specifies the minimum number of special characters the password must contain.
Permitted special characters	List of permitted special characters.
Max. identical characters in total	Specifies the maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Specifies the maximum number of identical character that can be repeated after each other.
Denied special characters	List of special characters that are not permitted.
Do not generate lowercase letters	Specifies whether a generated password can contain lowercase letters. This setting only applies when passwords are generated.
Do not generate uppercase letters	Specifies whether a generated password can contain uppercase letters. This setting only applies when passwords are generated.
Do not generate digits	Specifies whether a generated password can contain digits. This setting only applies when passwords are generated.
Do not generate special characters	Specifies whether a generated password can contain special characters. If this option is set, only letters, numbers, and spaces are allowed in passwords. This setting only applies when passwords are generated.

Custom scripts for password requirements

You can implement custom scripts for testing and generating passwords 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

- Checking passwords with a script on page 119
- Generating passwords with a script on page 120

Checking passwords with a script

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

Syntax of check scripts

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

With parameters:

`policy` = password policy object

`spwd` = password to check

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

Example: Script that checks a password

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

```
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. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
    a. In the Manager, select the **SAP R/3 > Basic configuration data > Password policies** category.
    b. In the result list, select the password policy.
    c. Select the **Change main data** task.
    d. On the **Scripts** tab, enter the name of the script to be used to check a password in the **Check script** field.
    e. (Optional) On the **Scripts** tab, in the **Additional requirements** field, enter the description of the additional requirements for the password that are checked by the script.
    f. Save the changes.

Related topics

- Generating passwords with a script on page 120

Generating passwords with a script

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 `Entity` property of the `PasswordPolicy` class.

Example: Script that generates a password

In random passwords, this script replaces the invalid characters **?** and **!** at the beginning of a password with _.

```
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. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
    a. In the Manager, select the **SAP R/3 > Basic configuration data > Password policies** category.
    b. In the result list, select the password policy.
    c. Select the **Change main data** task.
    d. On the **Scripts** tab, enter the name of the script to be used to generate a password in the **Generating script** field.
    e. Save the changes.

Related topics

- Checking passwords with a script on page 119

Password exclusion list

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. In the Designer, select the **Base data > Security settings > Password policies** category.
2. Create a new entry with the **Object > New** menu item and enter the term you want to exclude from the list.
3. Save the changes.

Checking a password

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

To verify if a password conforms to the password policy

1. In the Manager, select the **SAP R/3 > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
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 password generation

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. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Select the **Test** tab.
5. Click **Generate**.

   This generates and displays a password.

Initial password for new SAP user accounts

You can issue an initial password for a new SAP user account in the following ways:

- When you create the user account, enter a password in the main data.
- Assign a randomly generated initial password to enter when you create user accounts.
    - In the Designer, set the **TargetSystem | SAPR3 | Accounts | InitialRandomPassword** configuration parameter.
    - Apply target system specific password policies and define the character sets that the password must contain.
    - Specify which identity will receive the initial password by email.

Related topics

- Password policies for SAP user accounts on page 112
- Email notifications about login credentials on page 123

Email notifications about login credentials

Table 34: Configuration parameters for notifications about actions in the target system

Configuration parameter	Meaning
TargetSystem | SAPR3 | Accounts | InitialRandomPassword | SendTo	This configuration parameter specifies to which identity the email with the random generated password should be sent (manager cost center/department/location/business role, identity'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.
TargetSystem | SAPR3 | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Mail template name that is sent to supply users with the login credentials for the user account. The **Identity - new user account created** mail template is used.
TargetSystem | SAPR3 |	Mail template name that is sent to supply users with the

Configuration parameter	Meaning
Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	initial password. The **Identity - initial password for new user account** mail template is used.
TargetSystem | SAPR3 | DefaultAddress	Default email address of the recipient for notifications about actions in the target system.

You can configure the login credentials 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 text in a mail template is defined in several languages. This 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 credentials

1. Ensure that the email notification system is configured in One Identity Manager. For more information, see the *One Identity Manager Installation Guide*.
2. In the Designer, set the **Common | MailNotification | DefaultSender** configuration parameter and enter the sender address for sending the email notifications.
3. Ensure that all identities have a default email address. Notifications are sent to this address. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.
4. Ensure that a language can be determined for all identities. Only then can they receive email notifications in their own language. For more 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 identity.

To send initial login credentials by email

1. In the Designer, set the "TargetSystem | SAPR3 | Accounts | InitialRandomPassword" configuration parameter.
2. In the Designer, set the "TargetSystem | SAPR3 | Accounts | InitialRandomPassword | SendTo" configuration parameter and enter the message recipient as a value.
3. In the Designer, set the "TargetSystem | SAPR3 | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName" configuration parameter.

   By default, the message sent uses the "Identity - new user account created" mail template. The message contains the name of the user account.
4. In the Designer, set the "TargetSystem | SAPR3 | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword" configuration parameter.

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

TIP: To use custom mail templates for emails of this type, change the value of the configuration parameter.

5

SAP systems

NOTE: The Synchronization Editor sets up the SAP systems in the One Identity Manager database.

To edit an SAP system's main data

1. Select the **SAP R/3 > Systems** category.
2. Select an SAP system in the result list and run the **Change main data** task.
3. Edit the system's main data.
4. Save the changes.

Table 35: Main data for an SAP system

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

Related topics

- Providing system measurement data on page 215

SAP clients

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

To edit client main data

1. Select the **SAP R/3 > Clients** category.
2. Select the client in the result list. Select the **Change main data** task.
3. Edit the client's main data.
4. Save the changes.

General main data of SAP clients

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

Table 36: General main data of a client

Property	Description
Client no.	Number of the client.
Name	Client's name.
System	System to which the client belongs.
Canonical name	Client's canonical name.
Company	Company for which the client is set up. The company given here is used when a new user account is set up.
City	City where company resides.
Has user administration	Specifies whether the client is used for user administration. If this option is set, the most significant license of the user account is used for system measurement.

Property	Description
Account definition (initial)	Initial account definition for creating user accounts. This account definition is used if automatic assignment of identities 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 identity (**Linked**) if no account definition is given. This is the case on initial synchronization, for example. NOTE: If the CUA status **Child** is assigned, no account definition should be assigned.
Target system managers	Application role, in which target system managers are specified for the client. Target system managers only edit the objects from clients to which they are assigned. A different target system manager can be assigned to each client. 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.
Synchronized by	NOTE: You can only specify the synchronization type when adding a new client. No changes can be made after saving. If you create a client with the Synchronization Editor, **One Identity Manager** is used. Type of synchronization through which data is synchronized between the client and One Identity Manager. Once objects are available for this client in One Identity Manager, the type of synchronization can no longer be changed. If you create a client with the Synchronization Editor, One Identity Manager is used. **Table 37: Permitted values** Value: One Identity Manager — Synchronization by: SAP R/3 connector — Provisioned by: SAP R/3 connector Value: No synchronization — Synchronization by: none — Provisioned by: none NOTE: If you select **No synchronization**, you can define custom processes to exchange data between One Identity Manager and the target system.
ALE name	Name used to map the client as logical system in the SAP distribution model.

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	Text field for additional explanation.

Related topics

- Setting up account definitions on page 71
- Assigning account definitions to a target system on page 88
- Target system managers on page 96
- Special features of synchronizing with a CUA central system on page 36
- Excluding a child system from synchronization on page 38
- Providing system measurement data on page 215

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, user accounts can selectively inherit groups. To do this, groups and 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. Each table contains the category positions **position 1** to **position 63**.

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 the Manager, select the client in the **SAP R/3 > Clients** category.
2. Select the **Change main data** task.
3. Switch to the **Mapping rule category** tab.
4. Extend the relevant roots of a table.
5. To enable the category, double-click .
6. Enter a category name of your choice for user accounts and groups in the login language that you use.
7. Save the changes.

Detailed information about this topic

- SAP group, SAP role, and SAP profile inheritance based on categories on page 194
- One Identity Manager Target System Base Module Administration Guide

Editing synchronization projects

Synchronization projects in which a client is already used as a base object can also be opened in the 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: The Manager is locked for editing throughout. To edit objects in the Manager, close the Synchronization Editor.

To open an existing synchronization project in the Synchronization Editor

1. Select the **SAP R/3 > Clients** category.
2. Select the client in the result list. Select the **Change main data** task.
3. Select the **Edit synchronization project...** task.

Detailed information about this topic

- One Identity Manager Target System Synchronization Reference Guide

Related topics

- Customizing the synchronization configuration on page 40

7

SAP user accounts

You can manage SAP R/3 user accounts with One Identity Manager. 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 for or withdrawn from user accounts in One Identity Manager.

NOTE: The following user accounts are read into the One Identity Manager database during synchronization, but cannot be edited, created, or deleted in One Identity Manager.

- sap*
- sapcpic
- sapjsf
- ddic
- j2ee_admin
- j2ee_guest
- sladpiuser
- slddsuser
- adsuser
- ads_agent
- tmsadm
- earlywatch

Changes to these user accounts can only be made in SAP R/3 and transferred to the One Identity Manager by subsequent synchronization.

Detailed information about this topic

- Linking user accounts to identities on page 132
- Supported user account types on page 133
- Entering main data of SAP user accounts on page 138

Linking user accounts to identities

The main feature of One Identity Manager is to map identities together with the main data and permissions available to them in different target systems. To achieve this, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to identities. This provides an overview of the permissions for each identity in all of the connected target systems. One Identity Manager offers the option of managing user accounts and their permissions. You can provision modifications in the target systems. Identities 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, One Identity Manager offers different methods for supplying user accounts to identities. One Identity Manager supports the following methods for linking identities and their user accounts:

- Identities can automatically obtain their account definitions using user account resources.

  If an identity 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 identity using the integrated inheritance mechanisms and subsequent process handling.

  When you manage account definitions through user accounts, you can specify the way user accounts behave when identities are enabled or deleted.
- When user accounts are inserted, they can be automatically assigned to an existing identity or a new identity can be created if necessary. In the process, the identity main data is created on the basis of existing user account main 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. You must define criteria for finding identities for automatic identity assignment.
- Identities and user accounts can be entered manually and assigned to each other.

Related topics

- Entering main data of SAP user accounts on page 138
- Setting up account definitions on page 71
- Assigning identities automatically to SAP user accounts on page 160

For more information about identity 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 type

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

  Table 38: Identity types of user accounts

Identity type	Description	Value of the IdentityType column
Primary identity	Identity's default user account.	Primary
Organizational identity	Secondary user account used for different roles in the company, for example for subcontracts with other functional areas.	Organizational
Personalized administrator identity	User account with administrative permissions, used by an identity.	Admin
Sponsored identity	User account used for a specific purpose. For example, for training purposes.	Sponsored
Shared identity	User account with administrative permissions, used by multiple identities.	Shared
Service identity	Service account.	Service

- Privileged user account

  Privileged user accounts are used to provide identities with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are labeled with the **Privileged user account** property (`IsPrivilegedAccount` column).

Default user accounts

Normally, each identity obtains a default user account, which has the permissions they require for their regular work. The user accounts are linked to the identity. The effect of the

link and the scope of the identity'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 how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships at 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 IT operating data for user accounts and which default values are used if no IT operating data can be determined through an identity's primary roles.

   The type of IT operating data required depends on the target system. The following setting are recommended for default user accounts:

   - In the mapping rules for the `IsGroupAccount_SAPGrp`, `IsGroupAccount_SAPProfile`, and `IsGroupAccount_SAPRole` columns, use the default value **`1`** and set the **Always use default value** option.
   - 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 that IT operating data should apply when you set up a user account.
5. Assign the account definition to identities.

   When the account definition is assigned to an identity, 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, in the Designer, enable the **Mark selected user accounts as privileged** schedule.

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

- Personalized admin identity
  1. Link the user account to a pseudo identity using the `UID_Person` column.

     Use an identity with the same identity type or create a new identity.
  2. Assign this identity to hierarchical roles.
- Shared identity
  1. Assign all identities with usage authorization to the user account.
  2. Link the user account to a pseudo identity using the `UID_Person` column.

     Use an identity with the same identity type or create a new identity.
  3. Assign this pseudo identity to hierarchical roles.

  The pseudo identity provides the user account with its permissions.

Privileged user accounts

Privileged user accounts are used to provide identities with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are labeled with the **Privileged user account** property (`IsPrivilegedAccount` column).

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

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 are created.
3. Specify how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships in the manage level.
4. Create a formatting rule for the IT operating data.

   You use the mapping rule to define which rules are used to map IT operating data for user accounts and which default values are used if no IT operating data can be determined through an identity's primary roles.

   The type of IT operating data 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 set the **Always use default value** option.
   - 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_SAPGrp`, `IsGroupAccount_SAPProfile`, and `IsGroupAccount_SAPRole` columns with a default value of **`0`** and set the **Always use default value** option.

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 identities who work with privileged user accounts.

   When the account definition is assigned to an identity, 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, specify how the login names are formatted in the template.

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 for 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 roles or profiles from this client 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.

NOTE: In One Identity Manager, only SAP groups from the central system are mapped. SAP groups are not administered through the central user administration.

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

The access authorizations for central and child systems are read into theOne 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 an identity 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** field, select the **SAPUser** table. For more information, see Main data for an account definition on page 73.

   This account definition is required to generate a user account in the central system if the identity 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 39: Main data of an account definition for accessing clients

Property	Description
User account table	Select **SAPUserMandant** from the drop-down.
Target system	Client for which you want to grant access.
Required account definition	From the drop-down, select the account definition to generate user accounts in the central system. A user account is then created in the central system if the identity does not yet have a user account.
Manage level (initial)	Select **Unmanaged** from the drop-down.
Service item	Service item through which you can request the account definition resource in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Enable the option if access to the child system can be requested in the Web Portal.
Only for use in IT Shop	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.

   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 identity 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 155.

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

Detailed information about this topic

- Setting up account definitions on page 71

Related topics

- General main data of SAP clients on page 127
- Assigning SAP groups, SAP roles, and SAP profiles to SAP user accounts on page 177
- Inheriting SAP profiles and SAP roles in a central user administration on page 190
- Assigning identities automatically to SAP user accounts on page 160
- Removing a Central User Administration on page 229

Entering main data of SAP user accounts

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

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

NOTE: If identities are to obtain their user accounts through account definitions, the identities 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 the Manager, select the **SAP R/3 > User accounts** category.
2. Click in the result list.
3. On the main data form, edit the main data of the user account.
4. Save the changes.

To edit main data of a user account

1. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Edit the user account's resource data.
5. Save the changes.

To manually assign a user account for an identity

1. In the Manager, select the **Identities > Identities** category.
2. Select the identity in the result list.
3. Select the **Assign SAP user accounts** task.

4. Assign a user account.
5. Save the changes.

Detailed information about this topic

- General main data of an SAP user account on page 139
- SAP user account login data on page 144
- Phone numbers on page 146
- Fax numbers on page 147
- Email addresses on page 148
- Directly assigning SAP parameters on page 150
- Fixed values for an SAP user account on page 149
- Measurement data on page 150
- SNC data for an SAP user account on page 150

General main data of an SAP user account

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

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

Table 40: SAP user account address data

Property	Description
Identity	Identity that uses this user account. • An identity is already entered if the user account was generated by an account definition. • If you are using automatic identity assignment, an associated identity is found and added to the user account when you save the user account. • If you create the user account manually, you can select an identity in the drop-down. The drop-down displays activated and deactivated identities by default. If you do not want to see any deactivated identities, set the **QER | Person| HideDeactivatedIdentities** configuration parameter. NOTE: If you assign a deactivated identity to a user account, it might be locked or deleted depending on the configuration. You can create a new identity for a user account with an identity of

Property	Description
	type **Organizational identity**, **Personalized administrator identity**, **Sponsored identity**, **Shared identity**, or **Service identity**. To do this, click next to the input field and enter the required identity main data. Which login data is required depends on the selected identity type.
No link to an identity required	Specifies whether the user account is intentionally not assigned an identity. The option is automatically set if a user account is included in the exclusion list for automatic identity assignment or a corresponding attestation is carried out. You can set the option manually. Enable the option if the user account does not need to be linked with an identity (for example, if several identities use the user account). If attestation approves these user accounts, these user accounts will not be submitted for attestation in the future. In the Web Portal, user accounts that are not linked to an identity can be filtered according to various criteria.
Not linked to an identity	Indicates why the **No link to an identity required** option is enabled for this user account. Possible values: • **By administrator**: The option was set manually by the administrator. • **By attestation**: The user account was attested. • **By exclusion criterion**: The user account is not associated with an identity due to an exclusion criterion. For example, the user account is included in the exclude list for automatic identity assignment (configuration parameter **PersonExcludeList**).
Account definition	Account definition through which the user account was created. Use the account definition to automatically fill user account main data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned identity and enters it in the corresponding fields in the user account. NOTE: The account definition cannot be changed once the user account has been saved. NOTE: Use the user account's **Remove account definition** task to reset the user account to **Linked** status. This removes the account definition from both the user account and the identity. The user account remains but is not managed by the account definition anymore. The task only removes account definitions that are directly assigned (`XOrigin=1`).
Manage level	Manage level of the user account. Select a manage level from the

Property	Description
	drop-down. 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 drop-down.
Client	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.
User account	User account identifier. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. NOTE: Existing user accounts cannot be renamed.
User type	Type of user. Permitted values are: • User with classic address • Technical user • User with BP person • User with BP org and classic address • User with work center address
First name	The user's first name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Second name	User's second name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Last name	The user's last name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Second surname	The user's second surname.
Name at birth	The user's name at birth.
Surname prefix	User's last name prefix.
Second last name prefix	User's second last name prefix.
Form of address	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 mange level.
Academic title	Additional information about the user account.
Alias	Alternative ID for the user account that is used as log in for certain internet transactions.
Nickname	Additional information about the user account.

Property	Description
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 identity's name is represented in an extensively long form. The country serves to uniquely identify the formatting rule.
Country for name formatting	
ISO 639 - language	Default language for the user account according to ISO 639
Search pattern 1	Search pattern.
Search pattern 2	Search pattern.
Personnel number	SAP internal key for identifying an employee.
communications type	Unique identifier for the communications type
Company	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. NOTE: **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.
Risk index (calculated)	Maximum risk index value of all assigned groups, roles, and profiles. The property is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for the inheritance of groups, roles, and profiles by the user account. Groups, roles, and profiles can be selectively inherited by user accounts. To do this, groups, roles, and profiles and user accounts or contacts are divided into categories. Select one or more categories from the drop-down.
Identity type	User account's identity type Permitted values are: • **`Primary identity`**: Identity'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

Property	Description
	administrative permissions, used by one identity. • **Sponsored identity**: User account to use for a specific purpose. Training, for example. • **Shared identity**: User account with administrative permissions, used by several identities. Assign all identities that use this 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 through the linked identity. If the option is set, the user account inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests. • If you add an identity 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 identity has requested group membership in the IT Shop and the request is granted approval, the identity's user account only inherits the group if the option is set.
Profiles can be inherited	Specifies whether the user account can inherit profiles through the linked identity. If the option is set, the user account inherits profiles through hierarchical roles, in which the identity is a member, or through IT Shop requests.
Roles can be inherited	Specifies whether the user account can inherit SAP roles through the linked identity. If the option is set, the user account inherits the roles through hierarchical roles, in which the identity is a member, or through IT Shop requests.

Related topics

- Linking user accounts to identities on page 132
- Supported user account types on page 133
- Setting up account definitions on page 71
- Specifying categories for inheriting SAP groups, SAP roles, and SAP profiles on page 129
- General main data of SAP clients on page 127

Work center data for SAP user accounts

On the **Work center** tab, you can see all the work center data for a user account.

Table 41: SAP user account address data

Property	Description
Function	Additional information about the user account. Used when addresses are printed.
Department	Additional information about the user account. Used when addresses are printed.
Room in building	Additional information about the user account.
Floor	Additional information about the user account.
Building (number or token)	Additional information about the user account.

Related topics

- General main data of an SAP user account on page 139
- Entering main data of SAP user accounts on page 138

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 42: SAP user account login data

Property	Description
Password	Password for the user account. The identity's central password can be mapped to the user account password. For more information about an identity's central password, see *One Identity Manager Identity Management Base Module Administration Guide*. If you use a random generated initial password for the user accounts, it is automatically entered when a user account is created. The password is deleted from the database after publishing to the target system. NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password

Property	Description
	policy does not violate the target system's requirements.
Password confirmation	Reconfirm password.
Set effective password	Specifies whether the **Active password** password status is set if it is changed in the target system. NOTE: The effective password can only be set if the SAP R/3 connector for logging into the target system uses either SCN Login with single sign-on or an insecure connection.
Disabled password	Specifies whether the password is disabled (if single sign-on is used for logging in).
Security policy	Security policy for this user account.
User group	SAP group to use as user group for checking permissions.
Reference user	The user account contains authorizations for this reference user. A reference user is user account with the **Reference** user type. Use reference users to supply identical authorizations to different user accounts within one client.
Account is valid from	Validity period of the SAP user account.
Account is valid until	
Accounting number	Number for user account's accounting.
Cost center	Cost center for the user account's accounting.
User account type	Type of user account. The default user account type is specified in the **TargetSystem | SAPR3 | Accounts | Ustyp** configuration parameter.
User account locked	Specifies whether the user account is locked. If the user account is linked to an identity, the user account is unlocked when a new central password is set for the identity. This behavior is controlled by the **TargetSystem | SAPR3 | Accounts | UnlockByCentralPassword** configuration parameter. For more information about an identity's central password, see *One Identity Manager Identity Management Base Module Administration Guide*.
Last login	Date and time of last target SAP system login.

Related topics

- Password policies for SAP user accounts on page 112
- Initial password for new SAP user accounts on page 123
- Email notifications about login credentials on page 123
- User account types on page 99
- Locking and unlocking SAP user accounts on page 158
- Security policies on page 110

Phone numbers

You can edit user account email addresses on the **Phone numbers** tab.

To assign a phone number to a user account

1. Select the **Phone numbers** tab.
2. Click **Add**.

   This inserts a new row in the table.
3. Mark this row. Edit the telephone number main data.
4. Save the changes.

To edit a phone number

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

To remove a phone number assignment

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

Table 43: Phone number properties

Property	Description
Type	Type of phone connection Select either "Phone", "Phone (default)", "Mobile (default)" or "Mobile".

Property	Description
Country	Country for determining the country code.
Phone	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 mange level.
Phone number (complete)	Full phone number. Contains dialing code, connection, and extension numbers.
Preferred	Specifies the user's preferred telephone number.
Home address	Specifies whether this phone number is the user's home number.
SMS-enabled	Specifies whether text messages can be sent through this phone number.

Fax numbers

You can edit user account email addresses on the **Fax numbers** tab.

To assign a fax number to a user account

1. Select the **Fax numbers** tab.
2. Click **Add**.

   This inserts a new row in the table.
3. Mark this row. Edit the fax number main data.
4. Save the changes.

To edit a fax number

1. Select the **Fax numbers** tab.
2. Select the fax number in the list.
3. Edit the fax number main data.
4. Save the changes.

To remove a fax number assignment

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

Table 44: Fax numbers

Property	Description
Country	Country for determining the country code.
Fax number	Fax number with local area code. Enter an extension number in the extra field.
Fax number (complete)	Full fax number. Contains dialing code, connection, and extension numbers.
Preferred	Specifies the user's preferred fax number.
Home address	Specifies whether this fax number is the user's home number.

Email addresses

You can edit user account email addresses on the **Email addresses** tab.

To assign an email address to a user account

1. Select the **Email addresses** tab.
2. Click **Add**.

   This inserts a new row in the table.
3. Mark this row. Edit the email address main data.
4. Save the changes.

To edit an email address

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

To remove an email address assignment

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

Table 45: Email address data

Property	Description
Email address	Email address.

Property	Description
(SMTP)	
Email address search	Contains the first 20 characters of the email address in normalized form.
Preferred	Specifies the user's preferred email address.
Home address	Specifies the user's home address.

Fixed values for an SAP user account

Table 46: Configuration parameters for setting up user accounts

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

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

- In the Designer, set the configuration parameter values under "TargetSystem | SAPR3 | Accounts".

Measurement data

The license data for system measurement is shown on the **Measurement data** tab. For more information, see Providing system measurement data on page 215.

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 47: User account SNC data

Properties	Description
SNC Name	User account's SNC name. You can find the syntax for SNC names in the SNC user manual.
Login using SAP GUI allowed (insecure communication)	Specifies whether insecure communication is allowed for this user account.

Directly assigning SAP parameters

You can directly assign a user account parameter on the **Parameter** tab and specify its values. You can also see if a parameter is assigned directly, indirectly, or both ways.

To assign a parameter directly to user accounts

1. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list and run the **Change main data** task.
3. Select **Parameter**.
4. Click **Add**.

   This inserts a new row in the table.
5. Click to mark this row.
6. Select a parameter from the **Parameter** drop-down and specify a parameter value.
7. Save the changes.

To edit a parameter value

1. Select the **Parameter** tab.
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's direct assignment

1. Select the **Parameter** tab.
2. Select the parameter you want to remove.
3. If the parameter is only assigned directly, click **remove**.

   - OR -

   If the parameter is assigned both directly and indirectly, disable **Direct assignment**.
4. Save the changes.

Related topics

- SAP parameters on page 101
- Assigning SAP parameters to departments, cost centers, and locations on page 102
- Assigning SAP parameters to business roles on page 103
- Inheritance of parameter values by SAP user accounts on page 107

Additional tasks for managing SAP user accounts

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

Overview of SAP user accounts

To obtain an overview of a user account

1. Select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **SAP user account overview** task.

Changing the manage level of SAP user accounts

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

To change the manage level for a user account

1. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Select the manage level in the **Manage level** list on the **Address** tab.
5. Save the changes.

Related topics

- General main data of an SAP user account on page 139

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 done by allocating the identity, groups, and profiles to hierarchical roles such as departments, cost centers, locations, or business roles. If the identity 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. You cannot directly assign groups and profiles that have the **Only use in IT Shop** option set.

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 any clients assigned to this user account.

  Groups and profiles can also be directly assigned to a user account if the client's assignment to the user account is marked as outstanding. This removes the outstanding mark.

To assign groups and profiles directly to user accounts

1. Select the **SAP R/3 > User accounts** category.
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. In the **Add assignments** pane, assign the groups or profiles.

    - OR -

    In the **Remove assignments** pane, remove the groups or profiles.
5. Save the changes.

Related topics

- Assigning SAP groups, SAP roles, and SAP profiles to SAP user accounts on page 177

Assigning SAP roles directly to an SAP user account

Roles can be assigned directly or indirectly to a user account. Indirect assignment is done by allocating the identity and roles to hierarchical roles such as departments, cost centers, locations, or business roles. If the identity 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. You cannot directly assign roles that have the **Only use in IT Shop** option set.

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

NOTE: Roles can also be directly assigned to a user account if the client's assignment to the user account is marked as outstanding. This removes the outstanding mark.

To assign roles directly to user accounts

1. Select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign roles** task.

To assign a role

1. Click **Add**.

    This inserts a new row in the table.
2. Select the role you want to assign from the **Role** drop-down.

3. Enter a validity period for the role assignment in the **Valid from** and **Valid until** fields, 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 183

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 done by allocating the identity and structural profiles to hierarchical roles such as departments, cost centers, locations, or business roles. If the identity 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. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign structural profiles** task.

To assign a structural profile

1. Click **Add**.

   This inserts a new row in the table.
2. Select the structural profile to assign from the **Structural profile** drop-down.

3. If applicable, enter a validity period for the profile assignment in the **Valid from** and **Valid until** fields.
4. If the assignment temporarily is not active, set **Excluded**.
5. Assign more structural profiles as necessary.
6. Save the changes.

To edit a profile assignment

1. Select the profile assignment you want to edit in the table.
2. Edit the **Valid until** date or the **Excluded** option.
3. 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.

For more information about structural profiles, see the *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 136.

To react quickly to special requests, you can assign the clients directly to a user account. To do this, select the central system and the child system. Only SAP roles or profiles from this client 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 the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign access to clients** task.

To assign a client

1. Click **Add**.

   This inserts a new row in the table.
2. From the **Client** drop-down, 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.

Assigning SAP licenses

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

SAP licenses in child systems and in the central system can be assigned to user accounts for system measurement. For more information, see Providing system measurement data on page 215.

To assign licenses to a user account

1. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign SAP licenses in client systems** task.
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. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.

3. Select the **Assign SAP licenses in client systems** task.
4. Select an assignment in the table.
5. Edit the measurement data.
6. Save the changes.

To remove a license assignment

1. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign SAP licenses in client systems** task.
4. Select an assignment in the table.
5. Click **Delete**.
6. Save the changes.

The following license information is displayed on the form.

Table 48: Measurement data for a centrally administrated user account

Property	Description
Recipient client	Client containing the user account which is assigned a license. You can select the central system or a assigned child system.
License	User account license in the selected client.
License extension	License extension for the installed special version. Select the special version ID from the drop-down.
Country surcharge	Additional license fee.
Chargeable system	SAP system containing the client to be charged. This field is only shown if **`04 (substitute)`** or **`11 (Multi-client/system)`** is entered as the license.
Chargeable client	Client containing the user account to be charged. This field is only shown if **`04 (substitute)`** or **`11 (Multi-client/system)`** is entered as the license.
Chargeable user account	User account to be charged if **`04 (substitute)`** or **`11 (Multi-client/system)`** is entered as the license.
Substituted from	Time period in which another user account assumes responsibility. These fields are enabled if **`04 (substitute)`** is entered as the license.
Substituted until	

Related topics

- Special versions on page 111

Locking and unlocking SAP user accounts

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

To lock a user account

1. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Lock SAP user account** task.
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.

If the user account is linked to an identity, the user account is unlocked when a new central password is set for the identity. This behavior is controlled by the **TargetSystem | SAPR3 | Accounts | UnlockByCentralPassword** configuration parameter. For more information about an identity's central password, see *One Identity Manager Identity Management Base Module Administration Guide*.

To unlock a user account manually

1. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the SAP user account in the result list.
3. Select the **Unlock SAP user account** task.
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 166

Assigning extended properties to SAP user accounts

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

For more information about setting up extended properties, see the *One Identity Manager Compliance Rules Administration Guide*.

To specify extended properties for a user account

1. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

   TIP: In the **Remove assignments** pane, you can remove assigned extended properties.

   To remove an assignment

   - Select the extended property and double-click .
5. Save the changes.

Renaming SAP user accounts

You can rename user accounts by deleting them and recreating them under a different name. In this case, existing assignments are transferred to the new user account.

NOTE: User accounts with the **Full managed** manage level cannot be renamed.

To rename a user account

1. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Select the **Rename SAP user account** task.
5. Enter the new name of the user account and the initial password.
6. Click **OK**.

   This generates a process that publishes these changes to the target system.

Related topics

- Initial password for new SAP user accounts on page 123

Assigning identities automatically to SAP user accounts

Table 49: Configuration parameters for automatic identity assignment

Configuration parameter	Meaning
TargetSystem | SAPR3 | PersonAutoFullsync	Mode for automatic identity assignment for user accounts that are added to or updated in the database by synchronization.
TargetSystem | SAPR3 | PersonAutoDefault	Mode for automatic identity assignment for user accounts added to the database outside synchronization.
TargetSystem | SAPR3 | PersonExcludeList	Listing of all user account without automatic identity assignment. 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	Specifies whether identities are automatically assigned to disabled user accounts. User accounts are not given an account definition.

When you add a user account, an existing identity can automatically be assigned to it. If necessary, a new identity can be created. The identity main data is created on the basis of existing user account main data. This mechanism can be triggered after a new user account is created either manually or through synchronization.

Define criteria for finding identities to apply to automatic identity assignment. If a user account is linked to an identity 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 identities 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 identity assignments to user accounts remain intact.

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

For more information about assigning identities automatically, see the *One Identity Manager Target System Base Module Administration Guide*.

Run the following tasks to assign identities automatically.

- If you want identities to be assigned during the synchronization of user accounts, in the Designer, set the **TargetSystem | SAP3 | PersonAutoFullsync** configuration parameter and select the required mode.
- If you want identities to be assigned outside synchronization, in the Designer, set the **TargetSystem | SAP3 | PersonAutoDefault** configuration parameter and select the required mode.
- In the **TargetSystem | SAP3 | PersonExcludeList** configuration parameter, define the user accounts for which no automatic assignment to identities shall take place.

  Example:

  `SAP*|SAPCPIC|SAPJSF|DDIC|J2EE_ADMIN|J2EE_GUEST`

  TIP: You can edit the value of the configuration parameter in the **Exclude list for automatic identity assignment** dialog.

  To edit the exclude list for automatic identity assignment

  1. In the Designer, edit the **PersonExcludeList** configuration parameter.
  2. Click **...** next to the **Value** field.

     This opens the **Exclude list for SAP user accounts** dialog.
  3. To add a new entry, click **Add**.

     To edit an entry, select it and click **Edit**.
  4. Enter the name of the user account that does not allow identities to be assigned automatically.

     Each entry in the list is handled as part of a regular expression. You are allowed to use the usual special characters for regular expressions.
  5. To delete an entry, select it and click **Delete**.
  6. Click **OK**.
- Use the **TargetSystem | SAP3 | PersonAutoDisabledAccounts** configuration parameter to specify whether identities 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 identity assignment in the client.

NOTE:

The following applies for synchronization:

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

The following applies outside synchronization:

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

NOTE:

In the default installation, after synchronizing, identities are automatically created for the user accounts.If an account definition for the client is not known at the time of synchronization, user accounts are linked with identities. 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 manage user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the client.
3. Assign a user account in the **Linked** state to the account definition. The account definition's default manage level is applied to the user account.
    a. In the Manager, select the **SAP R/3 > User accounts > Linked but not configured > <client>** category.
    b. Select the **Assign account definition to linked accounts** task.
    c. In the **Account definition** drop-down, select the account definition.
    d. Select the user accounts that contain the account definition.
    e. Save the changes.

Related topics

- Creating an account definition on page 72
- Assigning account definitions to a target system on page 88
- Editing search criteria for automatic identity assignment on page 162

Editing search criteria for automatic identity assignment

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

The criteria for identity assignments are defined for the client. You specify which user account properties must match the identity's properties such that the identity 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 identity assignment** column (`AccountToPersonMatchingRule`) in the `SAPMandant` table.

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

NOTE: Object definitions for user accounts that can have search criteria applied to them are predefined. For example, if you require other objects definitions that limit a preselection of user accounts, set up the respective custom object definitions in the Designer. For more information, see the *One Identity Manager Configuration Guide*.

To specify criteria for identity assignment

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

Table 50: Standard search criteria for user accounts

Apply to	Identity column	User account column
SAP user accounts of the type "Dialog"	Central SAP user account (`CentralSAPAccount`)	User account (`Accnt`)

5. Save the changes.

Direct assignment of identities to user accounts based on a suggestion list

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

Table 51: Manual assignment view

View	Description
Suggested assignments	This view lists all user accounts to which One Identity Manager can assign an identity. All identities are shown that were found using the search criteria and can be assigned.
Assigned user accounts	This view lists all user accounts to which an identity is assigned.
No identity assignment	This view lists all user accounts to which no identity is assigned and for which no identity was found using the search criteria.

TIP: By double-clicking on an entry in the view, you can view the user account and identity main 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 identities directly using a suggestion list

1. Click **Suggested assignments**.
   a. Click **Selection** on all user accounts to which you want to assign the suggested identities. Multi-select is possible.
   b. Click **Assign selected.**
   c. Confirm the security prompt with **Yes**.

      The identities found using the search criteria are assigned to the selected user accounts.

   – OR –
2. Click **No identity assignment**.
   a. Click **Select identity** for the user account to which you want to assign an identity. Select an identity from the drop-down.
   b. Click **Selection** on all the user accounts to which you want to assign the selected identities. Multi-select is possible.
   c. Click **Assign selected**.
   d. Confirm the security prompt with **Yes**.

      The identities displayed in the **Identity** column are assigned to the selected user accounts
      .

To remove assignments

1. Click **Assigned user accounts**.
   a. Click **Selection** on all user accounts you want to delete the identity assignment from. Multi-select is possible.
   b. Click **Remove selected**.
   c. Confirm the security prompt with **Yes**.

      The assigned identities are removed from the selected user accounts.

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

Related topics

- Assigning identities automatically to SAP user accounts on page 160

Automatically creating departments based on SAP user account information

You can create new departments in One Identity Manager based on user accounts' department data. In addition, you can specify that departments of user account's identities are classified as the primary department. These identities can obtain their company resources through these assignments if One Identity Manager is configured correspondingly.

Prerequisites for using this method

- Identities must be created automatically when user accounts are added or modified. At least one of the following configuration parameters must be activated and the corresponding method implemented.

  Table 52: Configuration Parameter for automatic identity assignment

Configuration parameter	Effect when set
TargetSystem | SAPR3 | PersonAutoDefault	Based on the given mode, identities that were added to the database outside the synchronization are automatically assigned to user accounts.
TargetSystem | SAPR3 | PersonAutoFullsync	Based on the given mode, identities that were added to or updated in the database by synchronization are automatically assigned to user accounts.

- There is no synchronization project set up for personnel planning data.

  During synchronization of personnel planning data, departments that have been created already from SAP user account data are marked as outstanding. Use this method to automatically create departments from user account data only when departments are not added by synchronizing personnel planning data. For more information about synchronizing personnel planning data, see the *One Identity Manager Administration Guide for SAP R/3 Structural Profiles Add-on*.

To create departments from user account data

- In the Designer, enable the **TargetSystem | SAPR3 | AutoCreateDepartment** configuration parameter.

  For all departments imported into the One Identity Manager database in this way, **SAP R/3** is given as the data source for the import (column `ImportSource='SAP'`).

Related topics

- General main data of an SAP user account on page 139
- Assigning identities automatically to SAP user accounts on page 160

Locking SAP user accounts

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

Scenario: The user accounts are linked to identities and are managed through account definitions.

User accounts managed through account definitions are locked when the identity is temporarily or permanently disabled. The behavior depends on the user account manage level. Accounts with the **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` column.

Scenario: The user accounts are linked to identities. No account definition is applied.

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

- If the configuration parameter is set, the identity's user accounts are locked when the identity 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 identity'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 the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Lock user account** task.
4. Confirm the prompt with **OK**.

Scenario: The user accounts are not linked to identities.

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

1. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Lock user account** task.
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, the **User account locked**

option is enabled on the **Login data** tab. The user can no longer log in with this user account.

To unlock a user account

1. Select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Unlock user account** task.
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

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

Related topics

- Setting up account definitions on page 71
- Creating manage levels on page 75

Deleting and restoring SAP user accounts

As long as an account definition for an identity is valid, the identity retains the user account that was created by it. If the account definition assignment is removed, the user account that was created from this account definition, is deleted. User accounts marked as **Outstanding** are only deleted if the **QER | Person | User | DeleteOptions | DeleteOutstanding** configuration parameter is set.

In the Manager, you can delete a user account that was not created using an account definition in the result list or from the menu bar. After you have confirmed the security alert the user account is marked for deletion in the One Identity Manager.

To delete a user account

1. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Click to delete the user account.
4. Confirm the security prompt with **Yes**.

Deferred deletion is taken into account if a user account is being deleted. You can use deferred deletion to specify how long the user accounts remain in the database after

deletion is triggered before they are finally removed. You can reenable the user accounts up until deferred deletion runs.

If the **QER | Person | User | DeleteOptions | ReapplyTemplatesOnRestore** is set, the template is applied again when reenabling a user account marked for deletion that is managed through an account definition. This means that properties dependent on the IT operating data are automatically recreated according to the current configuration.

To restore a user account

1. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Click in the result list.

Configuring deferred deletion

You can use deferred deletion to specify how long the user accounts remain in the database after deletion is triggered before they are finally removed. By default, user accounts are finally deleted from the database after 30 days. First, the user accounts are disabled or locked. You can reenable the user accounts up until deferred deletion runs. After deferred deletion is run, the user accounts are deleted from the database and cannot be restored anymore.Deferred deletion has no influence over the login permission in assigned CUA child systems.

You have the following options for configuring deferred deletion.

- Global deferred deletion: Deferred deletion applies to user accounts in all target system. The default value is `30` days.

  In the Designer, enter a different value for deferred deletion in the `Deferred deletion [days]` property of the **SAPUser** table.
- Object-specific deferred deletion: Deferred deletion can be configured depending on certain properties of the accounts.

  To use object-specific deferred deletion, in the Designer, create a `Script (deferred deletion)` for the **SAPUser** table.

  Example: Script for object-specific deferred deletion

  Deferred deletion of privileged user accounts is 10 days. The following **Script (deferred deletion)** is entered in the table.

  ```
  If Not $IsPrivilegedAccount:Bool$ Then
       Value = 10
  End If
  ```

For more information on editing table definitions and configuring deferred deletion in the Designer, see the *One Identity Manager Configuration Guide*.

Entering external user IDs for SAP user accounts

External authentication methods for logging in 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.

To enter external IDs

1. Select the **SAP R/3 > External IDs** category.
2. Select the external identifier in the result list. Select the **Change main data** task.

   - OR -

   Click in the result list.
3. Enter the required data on the main data form.
4. Save the changes.

Enter the following data for an external identifier.

Table 53: External ID properties

Property	Description
External user ID	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. 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. • **`Distinguished Name for X.509`**: Login uses the distinguished name for X.509. • **`Windows NTLM or password verification with Windows domain controller`**: Login uses Windows NT Lan Manager or password verification with the Windows domain controller. • **`LDAP bind <user defined>`**: Login uses LDAP Bind (for other authentication mechanisms). • **`SAML Token`**: Authentication uses an SAML token profile.

Property	Description
	The default type is specified in the **TargetSystem | SAPR3 | Accounts | ExtID_Type** configuration parameter.
Target system type	Can be called up together with the external ID type to test the login data. The default type is specified in the **TargetSystem | SAPR3 | Accounts | TargetSystemID** configuration parameter. Permitted values are **ADSACCOUNT** and **NTACCOUNT**.
External user ID is enabled	Specifies whether the system can use the external user ID for the user to log in with an external authentication system.
User account	Assignment of the external user ID to a user account.
Sequential number	Sequential number, if a user account has more than one external identifiers.
Valid from	Date from which the external user ID is valid.

Related topics

- External identifier types on page 100

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 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 composite roles. Single roles can be grouped together into composite roles. User account member in the roles can be set for a limit period.

Profiles

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

Editing main data of 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 main data

1. Select the **SAP R/3 > Groups** category.
2. Select the group in the result list. Select the **Change main data** task.
3. Enter the required data on the main data form.
4. Save the changes.

To edit profile main data

1. Select the **SAP R/3 > Profiles** category.
2. Select a profile in the result list. Select the **Change main data** task.
3. Enter the required data on the main data form.
4. Save the changes.

To edit role main data

1. Select the **SAP R/3 > Roles** category.
2. Select the role in the result list. Select the **Change main data** task.
3. Enter the required data on the main data form.
4. Save the changes.

Detailed information about this topic

- General main data of SAP groups on page 172
- General main data of SAP roles on page 174
- General main data of SAP profiles on page 175

General main data of SAP groups

Table 54: Configuration parameters for risk assessment of SAP user accounts

Configuration parameter	Effect when set
QER | Calcu-lateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating the 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.

Edit the following main data of a group.

Table 55: SAP group main data

Property	Description
Display name	Name of the group as displayed in One Identity Manager tools. The group name is taken from the group identifier by default.
Name	Name of group in the target system.
Client	Client, in which the group is added.
Service item	Service item data for requesting the group through the IT Shop.
Risk index	Value for evaluating the risk of assigning the group to user accounts. Set a value in the range **0** to **1**. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is activated.
Category	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 drop-down.
Description	Text field for additional explanation.
IT Shop	Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested through the Web Portal and allocated by defined approval processes. The group can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested through the Web Portal and allocated by defined approval processes. Direct assignment of the group to hierarchical roles or user accounts is not permitted.

Detailed information about this topic

- Specifying categories for inheriting SAP groups, SAP roles, and SAP profiles on page 129
- 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 main data of SAP roles

Table 56: Configuration parameters for risk assessment of SAP user accounts

Configuration parameter	Effect when set
QER | CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating the 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.

Edit the following main data of a role.

Table 57: SAP role main data

Property	Description
Display name	Name of the role as displayed in One Identity Manager tools. Taken from the role identifier by default.
Name	Name of role in the target system.
Client	Client, in which the role is added.
License	Role license. This task is needed for finding system measurement for user accounts and is assigned once after synchronization.
Role type	Role type for differentiating between single and composite roles.
Service item	Service item data for requesting the role through the IT Shop.
Risk index	Value for evaluating the risk of assigning the role to user accounts. Enter a value between 0 and 1. This input field is only visible if the "QER | CalculateRiskIndex" configuration parameter is set.
Category	Categories for role inheritance. User accounts can inherit roles selectively. To do this, roles, and user accounts are divided into categories. Use this drop-down to allocate one or more categories to the role.
Description	Text field for additional explanation.
Role description	Text field for additional explanation.
IT Shop	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 user accounts and hierarchical roles.
Only for use in IT Shop	Specifies whether the role can only be requested through the IT Shop. This

Property	Description
	role can be requested by staff through the Web Portal and granted through a defined approval procedure. The role may not be assigned directly to hierarchical roles.

Detailed information about this topic

- Licenses on page 110
- Providing system measurement data on page 215
- Specifying categories for inheriting SAP groups, SAP roles, and SAP profiles on page 129
- 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 main data of SAP profiles

Table 58: Configuration parameters for risk assessment of SAP user accounts

Configuration parameter	Effect when set
QER | CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating the 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.

Edit the following main data of a profile.

Table 59: SAP profile main data

Property	Description
Display name	Name of the profile as displayed in One Identity Manager tools. The profile name is taken from the profile identifier by default.
Name	Name of profile in the target system.
Client	Client, in which the profile is added.
License	Profile license. This task is needed for finding system measurement for SAP user accounts and is assigned once after synchronization.

Property	Description
Profile type	Profile type for differentiating between single, composite, and generated profiles.
Service item	Service item data for requesting the profile through the IT Shop.
Risk index	Value for evaluating the risk of assigning the profile to account accounts. Enter a value between 0 and 1. This input field is only visible if the "QER | CalculateRiskIndex" configuration parameter is set.
Category	Category for profile inheritance. User accounts can selectively inherit profiles. To do this, profiles, and user accounts are divided into categories. Use this drop-down to allocate one or more categories to the profile.
Description	Text field for additional explanation.
Profile is enabled	Specifies whether the profile is enabled or a maintenance version.
Limited assignment	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.
IT Shop	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.
Only for use in IT Shop	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 be assigned directly to hierarchical roles. This option cannot be enabled for generated profiles.

Detailed information about this topic

- Licenses on page 110
- Providing system measurement data on page 215
- Specifying categories for inheriting SAP groups, SAP roles, and SAP profiles on page 129
- 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, identities, groups, roles, and profiles are arranged in hierarchical roles. The number of groups, roles, and profiles assigned to an identity is calculated from the position in the hierarchy and the direction of inheritance. If you add an identity to roles and that identity owns a user account, the user account is added to the group, role, or profile.

Furthermore, groups, roles, and profiles can be assigned to identities through IT Shop requests. Add identities 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 identities after approval is granted.

Prerequisites for indirect assignment of SAP groups to identity user accounts

- Assignment of identities and groups is permitted for role classes (departments, cost centers, locations, or business roles).
- User accounts are marked with the **Groups can be inherited** option.
- The user accounts and groups belong to the same SAP client.

Prerequisites for indirect assignment of SAP profiles to identity user accounts

- Assignment of identities and profiles is permitted for role classes (departments, cost centers, locations, or business roles).
- User accounts are labeled with the **Profiles can be inherited** option.
- The user accounts and profiles belong to the same SAP client.

  - OR -

  If the user accounts are managed through the Central User Administration, the user accounts have access permissions in the SAP clients to which the profiles belong.

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

Prerequisites for indirect assignment of SAP roles to identity user accounts

- Assignment of identities and roles is permitted for role classes (departments, cost centers, locations, or business roles).
- User accounts are labeled with the **Roles can be inherited** option.

- The user accounts and roles belong to the same SAP client.

  - OR -

  If the user accounts are managed through the Central User Administration, the user accounts have access permissions in the SAP clients to which the roles belong.

For more information see the following guides:

Topic	Guide
Basic principles for assigning and inheriting company resources	*One Identity Manager Identity Management Base Module Administration Guide* *One Identity Manager Business Roles Administration Guide*
Assigning company resources through IT Shop requests	*One Identity Manager IT Shop Administration Guide*
System roles	*One Identity Manager System Roles Administration Guide*

Detailed information about this topic

- Assigning SAP groups, SAP roles, and SAP profiles to organizations on page 178
- Assigning SAP groups, SAP roles, and SAP profiles to business roles on page 180
- Assigning SAP user accounts directly to SAP groups and SAP profiles on page 182
- Adding SAP groups, SAP roles, and SAP profiles to system roles on page 184
- Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 186
- Assignment and inheritance of SAP profiles and SAP roles to SAP user accounts on page 188
- Central user administration in One Identity Manager on page 136
- 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 the **SAP R/3 > Groups** category.
2. Select the group in the result list.

3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations.
    - 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 the **Remove assignments** pane.
5. Save the changes.

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

1. Select the **SAP R/3 > Roles** category.
2. Select the role in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations.
    - 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 the **Remove assignments** pane.
5. Save the changes.

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

1. Select the **SAP R/3 > Profiles** category.
2. Select a profile in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations.
    - 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 the **Remove assignments** pane.
5. Save the changes.

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

1. Select the **Organizations > Departments** category.

   - OR -

   Select the **Organizations > Cost centers** category.

   - OR -

   Select the **Organizations > Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign SAP groups** task.

   - OR -

   Select the **Assign SAP roles** task.

   - OR -

   Select the **Assign SAP profiles** task.
4. In the **Add assignments** pane, assign groups, roles, or profiles.

   - OR -

   In the **Remove assignments** pane, 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 180
- Assigning SAP user accounts directly to SAP groups and SAP profiles on page 182
- Adding SAP groups, SAP roles, and SAP profiles to system roles on page 184
- Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 186
- One Identity Manager users for managing SAP R/3 on page 12

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 the **SAP R/3 > Groups** category.
2. Select the group in the result list.

3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, assign business roles.

   - OR -

   In the **Remove assignments** pane, remove business roles.
5. Save the changes.

To assign a role to a business role (non role-based login)

1. Select the **SAP R/3 > Roles** category.
2. Select the role in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, assign business roles.

   - OR -

   In the **Remove assignments** pane, remove business roles.
5. Save the changes.

To assign a profile to a business role (non role-based login)

1. Select the **SAP R/3 > Profiles** category.
2. Select a profile in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, assign business roles.

   - OR -

   In the **Remove assignments** pane, remove business roles.
5. Save the changes.

To assign groups, roles, or profiles to a business role (non role-based login)

1. Select the **Business roles > <Role class>** category.
2. Select the business role in the result list.
3. Select the **Assign SAP groups** task.

   - OR -

   Select the **Assign SAP roles** task.

   - OR -

   Select the **Assign SAP profiles** task.
4. In the **Add assignments** pane, assign groups, roles, or profiles.

   - OR -

   In the **Remove assignments** pane, remove the groups, roles, or profiles.
5. Save the changes.

Related topics

- Assigning SAP groups, SAP roles, and SAP profiles to organizations on page 178
- Assigning SAP user accounts directly to SAP groups and SAP profiles on page 182
- Adding SAP groups, SAP roles, and SAP profiles to system roles on page 184
- Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 186
- One Identity Manager users for managing SAP R/3 on page 12

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
- A group or profile can also be directly assigned to a user account if the client's assignment to the user account is marked as outstanding. This removes the outstanding mark.

To assign a group directly to user accounts

1. Select the **SAP R/3 > Groups** category.
2. Select the group in the result list.
3. Select the **Assign user accounts** task.
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 the **SAP R/3 > Profiles** category.
2. Select a profile in the result list.
3. Select the **Assign user accounts** task.
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 152
- Assigning SAP groups, SAP roles, and SAP profiles to organizations on page 178
- Assigning SAP groups, SAP roles, and SAP profiles to business roles on page 180
- Adding SAP groups, SAP roles, and SAP profiles to system roles on page 184
- Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 186

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.

  NOTE: Roles can also be directly assigned to a user account if the client's assignment to the user account is marked as outstanding. This removes the outstanding mark.

To assign a role directly to user accounts

1. Select the **SAP R/3 > Roles** category.
2. Select the role in the result list.
3. Select the **Assign user accounts** task.

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 the **User account** drop-down.
3. Enter a validity period for the role assignment in the **Valid from** and **Valid until** fields, 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 153
- Assigning SAP groups, SAP roles, and SAP profiles to organizations on page 178
- Assigning SAP groups, SAP roles, and SAP profiles to business roles on page 180
- Adding SAP groups, SAP roles, and SAP profiles to system roles on page 184
- Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 186

Adding SAP groups, SAP roles, and SAP profiles to system roles

Installed modules: System Roles Module

Groups, roles, and profiles can be added to different system roles. If you assign a system role to identities, all SAP user accounts owned by these identities inherit the groups, roles, and profiles. 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 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 **SAP R/3 > Groups** category.
2. Select the group in the result list.
3. Select the **Assign system roles** task.

4. In the **Add assignments** pane, assign system roles.

   TIP: In the **Remove assignments** pane, you can remove the system role assignment.

   To remove an assignment

   - Select the system role and double-click ✓.

5. Save the changes.

To assign a role to system roles

1. Select the **SAP R/3 > Roles** category.
2. Select the role in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

   TIP: In the **Remove assignments** pane, you can remove the system role assignment.

   To remove an assignment

   - Select the system role and double-click ✓.

5. Save the changes.

To assign a profile to system roles

1. Select the **SAP R/3 > Profiles** category.
2. Select a profile in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

   TIP: In the **Remove assignments** pane, you can remove the system role assignment.

   To remove an assignment

   - Select the system role and double-click ✓.

5. Save the changes.

Detailed information about this topic

- SAP products on page 202

Related topics

- Assigning SAP groups, SAP roles, and SAP profiles to organizations on page 178
- Assigning SAP groups, SAP roles, and SAP profiles to business roles on page 180
- Assigning SAP user accounts directly to SAP groups and SAP profiles on page 182
- Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 186

Adding SAP groups, SAP roles, and SAP profiles to the IT Shop

NOTE: Only profiles that are not assigned to IT Shop roles can be assigned to SAP shelves.

When you assign a group, a role, or a profile to an 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 labeled with the **IT Shop** option.
- The group , the role or profile must be assigned a service item.

  TIP: In the 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 the Web Portal, assign a service category to the service item.
- If you only want the group, the role or profile to be assigned to identities 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 the IT Shop.

1. In the Manager, select the **SAP R/3 > Groups** or **SAP R/3 > Roles** or **SAP R/3 > Profiles** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > SAP groups** or **Entitlements > SAP roles** or **Entitlements > SAP profiles** (role-based login) category.
2. In the result list, select the group, the role or the profile.
3. Select the **Add to IT Shop** task.
4. To assign the group, role, or profile to shelves, select the **IT Shop shelves** tab and, in the **Add assignments** section, double-click on the shelves.
5. To assign the group, role, or profile to IT Shop templates, select the **IT Shoptemplates** tab and, in the **Add assignments** section, double-click on the templates.
6. Save the changes.

To remove a group, role, or profile from individual shelves of the IT Shop

1. In the Manager, select the **SAP R/3 > Groups** or **SAP R/3 > Roles** or **SAP R/3 > Profiles** (non role-based login) category.

   - OR -

In the Manager, select the **Entitlements > SAP groups** or **Entitlements > SAP roles** or **Entitlements > SAP profiles** (role-based login) category.

2. In the result list, select the group, the role or the profile.
3. Select the **Add to IT Shop** task.
4. To remove the group, role, or profile from the shelves, select the **IT Shop shelves** tab and, in the **Remove assignments** section, double-click the shelves.
5. To remove the group, role, or profile from the IT Shop templates, select the **IT Shop templates** tab and, in the **Remove assignments** section, double-click the templates.
6. Save the changes.

To remove a group, a role or profile from all shelves of the IT Shop

1. In the Manager, select the **SAP R/3 > Groups** or **SAP R/3 > Roles** or **SAP R/3 > Profiles** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > SAP groups** or **Entitlements > SAP roles** or **Entitlements > SAP profiles** (role-based login) category.
2. In the result list, select the group, the role or the profile.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

   The group , the role, or the 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 information about requesting company resources through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Related topics

- General main data of SAP groups on page 172
- Assigning SAP groups, SAP roles, and SAP profiles to organizations on page 178
- Assigning SAP groups, SAP roles, and SAP profiles to business roles on page 180
- Assigning SAP user accounts directly to SAP groups and SAP profiles on page 182
- Adding SAP groups, SAP roles, and SAP profiles to system roles on page 184

Assignment and inheritance of 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.

- Composite profiles can be put together from 0...n profiles or composite profiles. If a user account is assigned a composite profile, the target system only returns the user account membership in the assigned composite profile and not the membership in subprofiles.
- Single roles can put together from 0..n profiles. Only profiles that are not composite profiles can be assigned. Profiles that are assigned to a single role can no longer be assigned to a user account.
- Composite roles can be made up of 0...n single roles. Assignment of profiles or composite profiles to composite 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 identities.

In inheritance behavior:

- If a user account is assigned a composite role that owns single roles, the single roles are not added to the `SAPuserInSAPGroupTotal` table.
- If a user account is assigned a single role that owns profiles, the profiles are not added to the `SAPUserInSAPProfile` table.
- If a user account is assigned a single role and this single role is part of a composite role that is also assigned to this user account, the single role is not added to the `SAPUserInSAPRole` table under certain circumstances:
  - The validity period of both assignments is identical.

    - OR -

  - The **TargetSystem | SAPR3 | KeepRedundantProfiles** configuration parameter is not set.
- If a user account is assigned a composite profile with child profiles, the child profiles are not added to the `SAPUserInSAPProfile` table. If a child profile is additionally directly assigned to the user account, then the `SAPUserInSAPProfile` table also contains this direct assignment.

If a user account obtains additional roles or profiles through a reference user, these roles or profiles are only added in the `SAPUserInSAPRole` and `SAPUserInSAPProfile` tables for the reference user. When company resources assigned to an identity (`PersonHasObject` table) are calculated, the roles and profiles inherited by a user account through single roles, composite roles, composite profiles, and reference users are also taken into account.

Related topics

- Configuring single role assignment on page 189

Configuring single role assignment

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

The following applies by default for the inheritance of single roles by user accounts: If a single role is assigned to a user account and this single role is part of a composite role that is also assigned to the user account, then the assignment of the single role is additionally mapped in the `SAPUserInSAPRole` table if the validity period of the assigned single and composite role is not identical.

To prevent mapping of memberships in single roles in the `SAPUserInSAPRole` table if the single roles are part of assigned composite roles

- In the Designer, disable the **TargetSystem | SAPR3 | KeepRedundantProfiles** configuration parameter.

  The table contains only the membership in the composite role.

Effect of the KeepRedundantProfiles configuration parameter

A single role is assigned to a user account, as well as a composite role that contains this single role.

- The configuration parameter is set. Both role assignments have a different validity period.

  The `SAPUserInSAPRole` table contains both the composite role assignment and the single role assignment.

- The configuration parameter is set. Both role assignments have the same validity period.

  The `SAPUserInSAPRole` table contains only the assignment of the composite role.

- The configuration parameter is not set.

  The `SAPUserInSAPRole` table contains only the assignment of the composite role. This applies regardless of the validity period of either role assignment.

Related topics

- Assignment and inheritance of SAP profiles and SAP roles to SAP user accounts on page 188

Inheriting SAP profiles and SAP roles in a central user administration

If user accounts are managed through the central user administration, SAP roles and profiles can only inherited by user accounts if the user accounts have access permission for the client that the role and profiles belong to. By default, roles and profiles can only be inherited by user account if access to the clients is guaranteed explicitly. Otherwise, the roles and profiles are not inherited.

User accounts can be granted the missing client access automatically as soon as a role or profile is inherited by the client.

To automatically grant missing access permission to user accounts

- In the Designer, set the **TargetSystem | SAPR3 | AutoFillSAPUserMandant** configuration parameter.

The missing access permission is granted when inheritance is calculated (entry in the `SAPUserMandant` table) and the roles and profiles are assigned to the user accounts.

CAUTION: As inheritance is an automated process, user accounts can therefore be given access permission to clients without the target system owners knowing about it.

Related topics

- Central user administration in One Identity Manager on page 136
- Granting access to clients of a central user administration on page 155

Additional tasks for managing SAP groups, SAP roles, and SAP profiles

After you have entered the main 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 **SAP R/3 > Groups** category.
2. Select the group in the result list.

3. Select the **SAP group overview** task.

To obtain an overview of a profile

1. Select the **SAP R/3 > Profiles** category.
2. Select a profile in the result list.
3. Select the **SAP profile overview** task.

To obtain an overview of a role

1. Select the **SAP R/3 > Roles** category.
2. Select the role in the result list.
3. Select the **SAP role overview** task.

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 60: Configuration parameter for conditional inheritance

Configuration parameter	Effect when set
QER | Structures | Inherite | GroupExclusion	Preprocessor relevant configuration parameter for controlling effectiveness of group memberships. If the configuration parameter is set, memberships can be reduced on the basis of exclusion definitions. Changes to this configuration parameter require the database to be recompiled.

When groups are assigned to user accounts an identity 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 at any time either directly, indirectly, or with an IT Shop request. 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` tables by the `XIsInEffect` column.

Example: 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 "Marketing" department, group B through "Finance", and group C through the "Control group" business role.

Jo User1 has a user account in this client. They primarily belong to the "Marketing" department. The "Control group" business role and the "Finance" department are assigned to them 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 identity from being able to trigger a request and to pay invoices. That means, groups A, B, and C are mutually exclusive. An identity that checks invoices may not be able to make invoice payments as well. That means, groups B and C are mutually exclusive.

Table 61: Specifying excluded groups (`SAPGrpExclusion` table)

Effective group	Excluded group
Group A	
Group B	Group A
Group C	Group B

Table 62: Effective assignments

Identity	Member in role	Effective group
Pat Identity1	Marketing	Group A
Jan User3	Marketing, finance	Group B
Jo User1	Marketing, finance, control group	Group C
Chris User2	Marketing, control group	Group A, Group C

Only the group C assignment is in effect for Jo User1. It is published in the target system. If Jo User1 leaves the "control group" business role at a later date, group B also takes effect.

The groups A and C are in effect for Chris User2 because the groups are not defined as mutually exclusive. If this should not be allowed, define further exclusion for group C.

Table 63: Excluded groups and effective assignments

Identity	Member in role	Assigned group	Excluded group	Effective group
Chris User2	Marketing	Group A		Group C
	Control group	Group C	Group B	
			Group A	

Prerequisites

- The **QER | Structures | Inherite | GroupExclusion** configuration parameter is set.

  In the Designer, set the configuration parameter and compile the database.

  NOTE: If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

- Mutually exclusive groups, roles, and profiles belong to the same client.

To exclude a group

1. In the Manager, select the **SAP R/3 > Groups** category.
2. Select a group in the result list.
3. Select the **Exclude groups** task.
4. In the **Add assignments** pane, assign the groups that are mutually exclusive to the selected group.

   - OR -

   In the **Remove assignments** pane, remove the groups that are no longer mutually exclusive.
5. Save the changes.

To exclude roles

1. In the Manager, select the **SAP R/3 > Roles** category.
2. Select the role in the result list.
3. Select the **Exclude SAP roles** task.

   - OR -

   In the **Remove assignments** pane, remove the roles that are no longer mutually exclusive.
4. Save the changes.

To exclude profiles

1. In the Manager, select the category **SAP R/3 > Profiles**.
2. Select a profile in the result list.
3. Select the **Exclude roles** task.

   - OR -

   In the **Remove assignments** pane, remove the profiles that are no longer mutually exclusive.
4. Save the changes.

SAP group, SAP role, and SAP profile inheritance based on categories

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, user accounts can selectively inherit groups. To do this, groups and 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. Each table contains the category positions **position 1** to **position 63**.

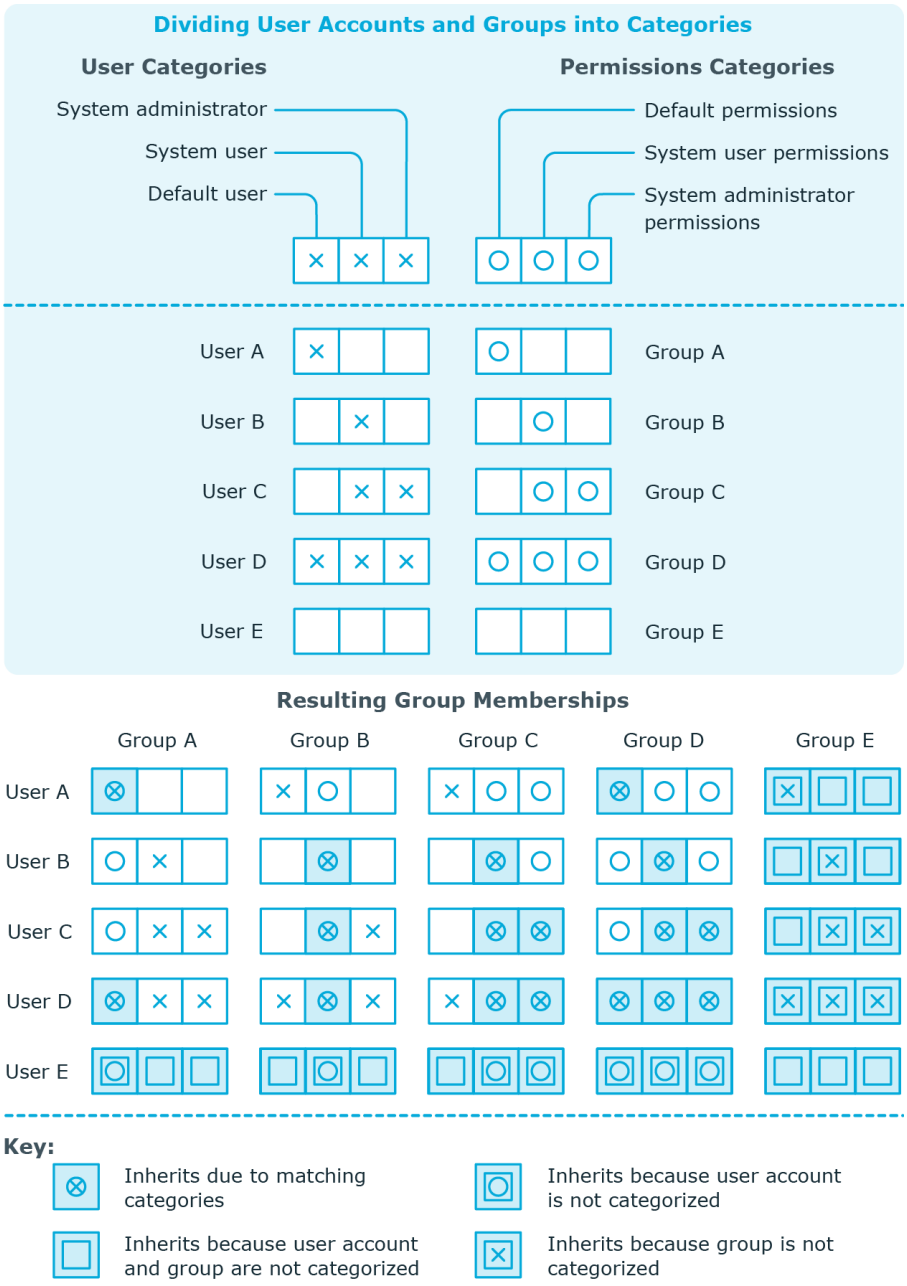
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or 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 64: Category examples

Category item	Categories for user accounts	Categories for groups
1	Default user	Default permissions
2	System users	System user permissions
3	System administrator	System administrator permissions

Figure 5: Example of inheriting through categories.



To use inheritance through categories

1. 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.

2. Assign categories to user accounts through their main data.
3. Assign categories to groups, roles, and profiles through their main data.

Related topics

- Specifying categories for inheriting SAP groups, SAP roles, and SAP profiles on page 129
- General main data of an SAP user account on page 139
- General main data of SAP groups on page 172
- General main data of SAP roles on page 174
- General main data of SAP profiles on page 175

Assigning extended properties to SAP groups, SAP roles, and SAP profiles

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

For more information about setting up extended properties, see the *One Identity Manager Compliance Rules Administration Guide*.

To specify extended properties for a group

1. In the Manager, select the **SAP R/3 > Groups** category.
2. Select the group in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

   TIP: In the **Remove assignments** pane, you can remove assigned extended properties.

   To remove an assignment

   - Select the extended property and double-click ✓.
5. Save the changes.

To specify extended properties for a role

1. In the Manager, select the **SAP R/3 > Roles** category.
2. Select the role in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

TIP: In the **Remove assignments** pane, you can remove assigned extended properties.

To remove an assignment

- Select the extended property and double-click .

5. Save the changes.

To specify extended properties for a profile

1. In the Manager, select the **SAP R/3 > Profiles** category.
2. Select a profile in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

   TIP: In the **Remove assignments** pane, you can remove assigned extended properties.

   To remove an assignment

   - Select the extended property and double-click .

5. Save the changes.

Showing SAP authorizations

You can view authorization objects and authorizations of One Identity Manager roles and profiles in SAP. All single profiles with their associated authorization objects and fields are displayed in a hierarchical overview.

To display role authorizations

1. Select the **SAP R/3 > Roles** category.
2. Select the role in the result list.
3. Select the **Show SAP authorizations** task.

To display profile authorizations

1. Select the **SAP R/3 > Profiles** category.
2. Select a profile in the result list.
3. Select the **Show SAP authorizations** task.

Validity period of role assignments

You can enter a validity period for assigning SAP roles to user accounts. If no validity period is given to the role assignments, they are allocated the following validity dates by default:

- Valid from: **1900-01-01**
- Valid to : **9999-12-31**

These role assignments are therefore unlimited.

The SAPUserInSAPRole table contains all role assignments, limited, and unlimited.

The HelperSAPUserInSAPRole table only contains current valid role assignments. The **Daily calculation of SAP user accounts assignments to SAP roles** schedule controls the calculation of this table.

Detailed information about this topic

- Assigning the validity period of direct role assignments on page 198
- Configuring the validity period of indirect role assignments on page 199
- Determining the validity period of indirect role assignments on page 200

Related topics

- Assigning SAP roles directly to an SAP user account on page 153
- Assigning SAP user accounts directly to SAP roles on page 183

Assigning the validity period of direct role assignments

Direct assignments can occur in two different ways:

a. Synchronizing role assignments

   The **Valid from** and **Valid to** columns are taken into account in the default mapping. Synchronization writes the validity period of role assignments into the One Identity Manager database.

b. Direct assignment of SAP roles to user accounts in the Manager

   A validity period can be entered for direct assignment of SAP roles to user accounts. **Valid from** and **Valid to** dates are provisioned in the target system.

Related topics

- Determining the validity period of indirect role assignments on page 200
- Validity period of role assignments on page 197

Configuring the validity period of indirect role assignments

When the validity period is calculated, the following configuration parameters are taken into account. These configuration parameters are disabled by default.

- **TargetSystem | SAPR3 | ValidDateHandling | DoNotUsePWODate**

  Specifies whether the request's validity period is transferred when role assignments are requested.

  Not set: The request's validity period is transferred. If there is no validity period given, the default values of **1900-01-01** and **9999-12-31** are set.

  Set: The role assignment is unlimited.

- **TargetSystem | SAPR3 | ValidDateHandling | ReuseInheritedDate**

  Controls reuse of existing profile assignments if another assignment for the same combination of user account and SAP role is added.

  Set: Existing role assignments are reused if the same assignment is created by different means of inheritance. The following applies:

  - The **Valid from** date of the existing assignment is in the past.
  - The **Valid until** date of the existing assignment is **9999-12-31** or the new assignment has the same **Valid until** date as the existing assignment.

  Any other unlimited assignment or any other assignment with the same **Valid until** date does not generate a new entry in the `SAPUserInSAPRole` table. This can reduce the number of entries in the `SAPUserInSAPRole` table.

  Not set: An entry in the `SAPUserInSAPRole` table is created for every new role assignment. Existing assignments are not reused.

  > NOTE: In databases that are migrated from versions older than 7.0, you may see assignments with a **Valid until** date of **9998-12-31**. This is a valid date for unlimited role assignments, which means that these assignments can also be reused.

- **TargetSystem | SAPR3 | ValidDateHandling | ReuseInheritedDate | UseTodayForInheritedValidFrom**

  Specifies the value that indirect role assignments' **Valid from** date contain when they are added.

  Not set: **1900-01-01**

  Set: **<today>**

  > 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 the information about when a role assignment's validity period starts is not absolutely necessary in SAP R/3.

To reuse an existing role assignment:

- In the Designer, set the **TargetSystem | SAPR3 | ValidDateHandling | ReuseInheritedDate** configuration parameter.

To set the assignment's date as the first day of the role assignment's validity period

- In the Designer, set the **TargetSystem | SAPR3 | ValidDateHandling | ReuseInheritedDate | UseTodayForInheritedValidFrom** configuration parameter.

To prevent the request's validity date being copied to the role assignment

- In the Designer, set the **TargetSystem | SAPR3 | ValidDateHandling | DoNotUsePWODate** configuration parameter.

  This adds an unlimited role assignment.

Related topics

- Determining the validity period of indirect role assignments on page 200

Determining the validity period of indirect role assignments

SAP roles that are assigned to departments, cost centers, locations, or business roles are indirectly assigned through them to user accounts. By default, indirect assignments are unlimited. The **TargetSystem | SAPR3 | ValidDateHandling** configuration parameter is used to determine the validity period of indirect assignments.

You can enter a valid from date if the requests are made in the IT Shop. An entry in `SAPUserInSAPRole` only exist between the first and last days of the request's validity period. The request's validity period is copied to role assignments under the following prerequisites:

- The **DoNotUsePWODate** configuration parameter is not set (default).
- The SAP role was requested directly.

  - OR -
- The assignment was created through an assignment request and at the same time a role assignment was requested. `BaseTreeHasSAPRole.XOrigin='8'` is set for this.

By default, an entry in the `SAPUserInSAPRole` table is created for every new role assignment. If the same assignment is created by different means of inheritance, the number of entries in the `SAPUserInSAPRole` table grows rapidly. In this case, if the validity period is identical, the same entries can be reused. Existing role assignments can be reused under the following prerequisites:

- The **ReuseInheritedDate** configuration parameter is set.

- The **Valid from** date of the existing assignment is in the past.
- The **Valid until** date of the existing assignment is **9999-12-31** or the new assignment has the same **Valid until** date as the existing assignment.
- Another assignment for the same combination of user account and SAP role is added.

Any other unlimited assignment or any other assignment with the same **Valid until** date does not generate a new entry in the SAPUserInSAPRole table. The number of entries in the SAPUserInSAPRole table can be reduced in this way.

NOTE: In databases that are migrated from versions older than 7.0, you may see assignments with a **Valid until** date of **9998-12-31**. This is a valid date for unlimited role assignments, which means that these assignments can also be reused.

By default, the first day that indirect assignments are valid is **1900-01-01**. This does not tell us when the assignments were created. If you need this information, in the **Valid from** field, you can enter the date on which the SAP role will be assigned. The date of the assignment is set as the first valid day of the indirect role assignments under the following prerequisites:

- The **ReuseInheritedDate | UseTodayForInheritedValidFrom** configuration parameter is set.

  Exception: the **DoNotUsePWODate** configuration parameter is not set and:
  - The assignment has been requested and the request has a **Valid from** date.
  - The assignment has been requested and the request has a **Valid to** date but no **Valid from** date.

IMPORTANT: Calculating indirect role assignments can become much slower depending on the amount of data to be processed.

Do not set the **UseTodayForInheritedValidFrom** configuration parameter if the information about the valid from date of the role assignment is not absolutely necessary in SAP R/3!

Detailed information about this topic

- Configuring the validity period of indirect role assignments on page 199
- Validity period of role assignments on page 197

Related topics

- Assigning the validity period of direct role assignments on page 198

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". Identities can obtain SAP products directly, inherit them though hierarchical role, or request them in the IT Shop.

The identity'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 the **SAP R/3 > Products** category.
2. Select an SAP product in the result list.

   – OR –

   Click in the result list.

   This opens the main data form for a system role.
3. Edit the system role's main data.
4. Save the changes.

For more information about system roles, see the *One Identity Manager System Roles Administration Guide*.

General main data of SAP products

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

Configuration parameter	Effect when set
QER | CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating the 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.

Enter the following data for a system role.

Table 66: System role main data

Property	Description
Display name	Name for displaying the system roles in One Identity Manager tools.
System role	Unique identifier for the system role.
Internal product name	An additional internal name for the system role.
System role type	Specifies the type of company resources, which comprise the system role.
Service item	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*.
System role manager	Manager responsible for the system role. Assign any identity. This identity can edit system role main 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.
Share date	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. Identities 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 controlled with the **Disabled** option in these cases. NOTE: Configure and enable the **Share system roles** schedule in the

Property	Description
	Designer to check the share date. For more information about schedules, see the *One Identity Manager Operational Guide*.
Risk index (calculated)	Maximum risk index values for all company resources. The property is only visible if the **QER | CalculateRiskIndex** configuration parameter is enabled. For more information about calculating the risk index, see the *One Identity Manager Risk Assessment Administration Guide*.
Comment	Text field for additional explanation.
Remarks	Text field for additional explanation.
Description	Text field for additional explanation.
Deactivated	Specifies whether identities and workdesks inherit the company resources contained in the system role. If this option is set, the system role can be assigned to identities, 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.
IT Shop	Specifies whether the system role can be requested through the IT Shop. The system role can be requested through the Web Portal and allocated by defined approval processes. The system role can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only for use in IT Shop	Specifies whether the system role can only be requested through the IT Shop. The system role can be requested through the Web Portal and allocated by defined approval processes. The system role may not be assigned directly to hierarchical roles.
Spare field no. 01 ... Spare field no. 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

For more information about system roles, see the *One Identity Manager System Roles Administration Guide*.

Assigning SAP products to identities

SAP products can be assigned directly or indirectly to identities. In the case of indirect assignment, identities and SAP products are arranged in hierarchical roles. The number of

SAP products assigned to an identity is calculated from the position in the hierarchy and the direction of inheritance.

If you add an identity to roles and that identity owns a user account, the user account is added to all groups, roles, or profiles included in the SAP products owned by the identity. The groups, roles, or profiles are not inherited if the SAP product is disabled or if the share date is still in the future.

Furthermore, SAP products can be assigned to identities through IT Shop requests. SAP products can be assigned through IT Shop requests by adding identities 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 identities after approval is granted.

Prerequisites for indirect assignment of SAP groups, roles, and profiles through SAP products to user accounts are:

- Assignment of system roles, identities, groups, roles, and profiles is permitted for role classes (departments, cost centers, locations, or business roles).
- The user accounts are labeled with the **Groups can be inherited**, **Profiles can be inherited**, and **Roles can be inherited** options.
- The user accounts, groups, roles, and profiles belong to the same SAP client.

For more information see the following guides:

Topic	Guide
Basic principles for assigning and inheriting company resources	*One Identity Manager Identity Management Base Module Administration Guide* *One Identity Manager Business Roles Administration Guide*
Assigning company resources through IT Shop requests	*One Identity Manager IT Shop Administration Guide*
System roles	*One Identity Manager System Roles Administration Guide*

Detailed information about this topic

- Assigning SAP products to organizations on page 206
- Assigning SAP products to business roles on page 206
- Assigning SAP products directly to identities on page 207
- Adding SAP products to system roles on page 207
- Adding SAP products to the IT Shop on page 208

Related topics

- Assigning SAP groups, SAP roles, and SAP profiles to SAP user accounts on page 177

Assigning SAP products to organizations

Assign SAP products to departments, cost centers, and locations in order to assign identities to them through these organizations.

To assign an SAP product to departments, cost centers, or locations

1. Select the **SAP R/3 > Products** category.
2. Select the SAP product in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
   - On the **Departments** tab, assign departments.
   - On the **Locations** tab, assign locations.
   - Assign cost centers on the **Cost centers** tab.

   - OR -

   Remove the organizations in the **Remove assignments** pane.
5. Save the changes.

Related topics

- Assigning SAP products to business roles on page 206
- Adding SAP products to the IT Shop on page 208
- Assigning SAP products directly to identities on page 207
- Adding SAP products to system roles on page 207
- Assigning SAP groups, SAP roles, and SAP profiles to organizations on page 178

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 the **SAP R/3 > Products** category.
2. Select the SAP product in the result list.
3. Select the **Assign business roles** task.

4. In the **Add assignments** pane, assign business roles.

   - OR -

   In the **Remove assignments** pane, remove business roles.
5. Save the changes.

Related topics

- Assigning SAP products to organizations on page 206
- Adding SAP products to system roles on page 207
- Assigning SAP products directly to identities on page 207
- Adding SAP products to the IT Shop on page 208
- Assigning SAP groups, SAP roles, and SAP profiles to business roles on page 180

Assigning SAP products directly to identities

You can assign SAP products directly to identities. All groups, roles, and profiles are assigned to this SAP product can be inherited by these identities.

To assign an SAP product directly to identities

1. Select the **SAP R/3 > Products** category.
2. Select the SAP product in the result list.
3. Select the **Assign to identities** task.
4. In the **Add assignments** pane, assign identities.

   - OR -

   In the **Remove assignments** pane, remove identities.
5. Save the changes.

Related topics

- Assigning SAP products to organizations on page 206
- Assigning SAP products to business roles on page 206
- Adding SAP products to the IT Shop on page 208
- Adding SAP products to system roles on page 207

Adding SAP products to 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 the **Only use in IT Shop** option enabled can only be assigned to system roles that also have this option set.

To assign an SAP product to system roles

1. Select the **SAP R/3 > Products** category.
2. Select the SAP product in the result list.
3. Select the **Assign system roles** task.
4. Select the **System role contained in** tab to assign parent system roles.
    - In the **Add assignments** pane, assign system roles.

      - OR -

      In the **Remove assignments** pane, remove system roles.
5. Select the **System role contains** tab to assign child system roles.
    - In the **Add assignments** pane, assign system roles.

      - OR -

      In the **Remove assignments** pane, remove system roles.
6. Save the changes.

Related topics

- Assigning SAP products to organizations on page 206
- Assigning SAP products to business roles on page 206
- Assigning SAP products directly to identities on page 207
- Adding SAP products to the IT Shop on page 208
- Adding SAP groups, SAP roles, and SAP profiles to system roles on page 184

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 SAPproduct must be labeled with **IT Shop**the 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 identities 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 the **SAP R/3 > Products** category.
2. Select the SAP product in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, 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 the **SAP R/3 > Products** category.
2. Select the SAP product in the result list.
3. Select **Add to IT Shop**.
4. In the **Remove assignments** pane, 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 the **SAP R/3 > Products** category.
2. Select the SAP product in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
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 information about providing products in the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Related topics

- Assigning SAP products directly to identities on page 207
- Assigning SAP products to organizations on page 206
- Adding SAP products to system roles on page 207
- Assigning SAP products to business roles on page 206
- Adding SAP groups, SAP roles, and SAP profiles to the IT Shop on page 186

Additional tasks for managing SAP products

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

Overview of SAP products

To obtain an overview of an SAP product

1. Select the **SAP R/3 > Products** category.
2. Select the SAP product in the result list.
3. Select the **System role overview** task.

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. Identities 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 the **SAP R/3 > Products** category.
2. Select the SAP product in the result list.
3. Select the **Assign SAP groups** task.
4. In the **Add assignments** pane, assign groups.

   - OR -

   In the **Remove assignments** pane, remove the groups.
5. Save the changes.

To assign profiles to an SAP product.

1. Select the **SAP R/3 > Products** category.
2. Select the SAP product in the result list.
3. Select the **Assign SAP profiles** task.

4. In the **Add assignments** pane, assign profiles.

   - OR -

   In the **Remove assignments** pane, remove the profiles.
5. Save the changes.

To assign roles to an SAP product

1. Select the **SAP R/3 > Products** category.
2. Select the SAP product in the result list.
3. Select the **Assign SAP roles** task.
4. In the **Add assignments** pane, assign roles.

   - OR -

   In the **Remove assignments** pane, remove the roles.
5. Save the changes.

Related topics

- Assigning SAP products to identities on page 204

Assigning SAP parameter to SAP products

Use this task to add parameters to an SAP product. If you assign the SAP product to identities, the parameters contained in the SAP product are inherited by the identities.

To assign parameters to an SAP product

1. Select the **SAP R/3 > Products** category.
2. Select the SAP product in the result list.
3. Select the **Assign SAP parameters** task.
4. In the **Add assignments** pane, assign parameters.

   - OR -

   In the **Remove assignments** pane, remove parameters.
5. Save the changes.

Detailed information about this topic

- SAP parameters on page 101

Assigning account definitions to SAP products

Use this task to add account definitions to an SAP product. If you assign the SAP product to identities, the account definitions contained in the SAP product are inherited by the identities.

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 the **SAP R/3 > Products** category.
2. Select the SAP product in the result list.
3. Select the **Assign account definitions** task.
4. In the **Add assignments** pane, assign account definitions.

   - OR -

   In the **Remove assignments** pane, remove the account definitions.
5. Save the changes.

Detailed information about this topic

- Setting up account definitions on page 71

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 identities, the subscribable reports contained in the SAP product are inherited by the identities.

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 the **SAP R/3 > Products** category.
2. Select the SAP product in the result list.
3. Select the **Assign subscribable reports** task.

4. In the **Add assignments** pane, assign subscribable reports.

   - OR -

   In the **Remove assignments** pane, remove the subscribable reports.
5. Save the changes.

Detailed information about this topic

- One Identity Manager Report Subscriptions Administration Guide

Assigning extended properties to SAP products

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

For more information about setting up extended properties, see the *One Identity Manager Compliance Rules Administration Guide*.

To specify extended properties for an SAP product

1. In the Manager, select the category **SAP R/3 > Products**.
2. Select the SAP product in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

   TIP: In the **Remove assignments** pane, you can remove assigned extended properties.

   To remove an assignment

   - Select the extended property and double-click .
5. Save the changes.

Editing conflicting system roles

Table 67: Configuration parameters for editing mutually exclusive roles

Configuration parameter	Effect when set
QER | Structures | Inherite | ESetExclusion	Preprocessor-relevant configuration parameter for defining the effectiveness of system roles If this parameter is set, mutually excluding system roles can be defined. Changes to this parameter require the database to be recompiled.

Configuration parameter	Effect when set
	If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

It is possible that identities 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 identity. Definitions made on parent or child SAP products do not affect the assignment.

To implement conflicting system roles

- In the Designer, set the **QER | Structures | Inherite | ESetExclusion** configuration parameter and compile the database.

  NOTE: If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

To define conflicting system roles

1. In the Manager, select the category **SAP R/3 > Products**.
2. Select the SAP product in the result list for which you want to define conflicting system roles.
3. Select the **Edit conflicting system roles** task.
4. In the **Add Assignments** panes, double-click the system roles are mutually exclusive to the selected SAP product.

   - OR -

   In the **Remove assignments** pane, remove 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 identity can have several user accounts which belong to different clients and systems. The identity'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 identity'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. In the Designer, set the **TargetSystem | SAPR3 | Accounts | CalculateLicence** configuration parameter.
2. In SAP, set the **Enable system measurement** option.
3. Set **Has user administration** in the client.
4. 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.
5. 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 126
- General main data of SAP clients on page 127
- Finding licenses using SAP roles and SAP profiles on page 219
- Entering licenses for SAP user accounts on page 218
- Transferring calculated licenses on page 222

Mapping the measurement data

Measurement data is displayed on the main data form for user accounts which are not CUA.

To display measurement data

1. Select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Change to **Inventory data**.

   This open the main data form with synchronized and calculated data for system measurement.

The following license information is displayed on the form.

Table 68: User account measurement data

Property	Description
Active License	User account's license. The active license is loaded into the One Identity Manager database by synchronization or found from the calculated, identity-related license. NOTE: The active license can also be edited 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. 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.
Special version ID	License extension for the installed special version. Select the special version ID from the drop-down. This is only enabled if special versions are permitted for the active license.
Country surcharge	Additional license fee. This is only enabled if country surcharges are permitted for the active license.
Substitute	Link to the user account which takes over as deputy for a specified time

Property	Description
	period. This field is only active if "04 (substitute)" or "11 (Multi-client/system)" is entered. The substitute user account obtains roles and profiles of the displayed user account for a specified time period.
Substituted from	Time period in which another user account assumes responsibility. This input field is enabled if the active license is set to "04 (substitute)".
Substituted until	
Calculated license (client)	License determined from user account assigned roles and profiles within the client. This field is only visible if the **TargetSystem | SAPR3 | Accounts | CalculateLicence** configuration parameter, the **System measurement enabled** option in SAP, and the **Has user administration** option in the SAP client are enabled.
Calculated license (identity)	License of most significant identity user account. The client related calculated license is entered for the most significant user account. For all the other identity's user accounts, the identity related calculated license "11 (Multi-client/system user)" is entered. This also contains a reference to the calculated most significant user account (**Calculated ref. name**). This field is only visible if the **TargetSystem | SAPR3 | Accounts | CalculateLicence** configuration parameter, the **System measurement enabled** option in SAP, and the **Has user administration** option in the SAP client are enabled.
Calculated ref.name	Link to the calculated most significant user account if "11 (Multi-client/system user)" is entered. This field is only visible if the **TargetSystem | SAPR3 | Accounts | CalculateLicence** configuration parameter, the **System measurement enabled** option in SAP, and the **Has user administration** option in the SAP client are enabled.

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. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign SAP licenses in client systems** task.
4. Select an assignment in the table.

The following license information is displayed on the form.

Table 69: Measurement data for a centrally administrated user account

Property	Description
Recipient client	Client containing the user account which is assigned a license. You can select the central system or a assigned child system.
License	User account license in the selected client.
License extension	License extension for the installed special version. Select the special version ID from the drop-down.
Country surcharge	Additional license fee.
Chargeable system	SAP system containing the client to be charged. This field is only shown if **04 (substitute)** or **11 (Multi-client/system)** is entered as the license.
Chargeable client	Client containing the user account to be charged. This field is only shown if **04 (substitute)** or **11 (Multi-client/system)** is entered as the license.
Chargeable user account	User account to be charged if **04 (substitute)** or **11 (Multi-client/system)** is entered as the license.
Substituted from	Time period in which another user account assumes responsibility. These fields are enabled if **04 (substitute)** is entered as the license.
Substituted until	

Related topics

- Entering licenses for SAP user accounts on page 218
- Finding licenses using SAP roles and SAP profiles on page 219
- Determining an SAP user account rating on page 220
- Transferring calculated licenses on page 222
- Special versions on page 111
- Licenses on page 110

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 the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.

3. Select the **Measurement data** tab.
4. Select a license in the **Active license** drop-down.
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. In the Manager, select the **SAP R/3 > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign SAP licenses in client systems** task.
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 216
- Finding licenses using SAP roles and SAP profiles on page 219

Finding 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 identity'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 the **SAP R/3 > Roles** category.

   – OR –

   Select the **SAP R/3 > Profiles** category.

2. Select the role or profile in the result list.
3. Assign a license in the **License** field.
4. Save the changes.

Related topics

- Licenses on page 110
- General main data of SAP profiles on page 175
- General main data of SAP roles on page 174

Determining an SAP user account rating

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:

- The **TargetSystem | SAPR3 | Accounts | CalculateLicence** configuration parameter is set
- The **System measurement enabled** option for the SAP system is disabled/enabled
- The **Has user account management** option 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
- Identity 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 (identity related)

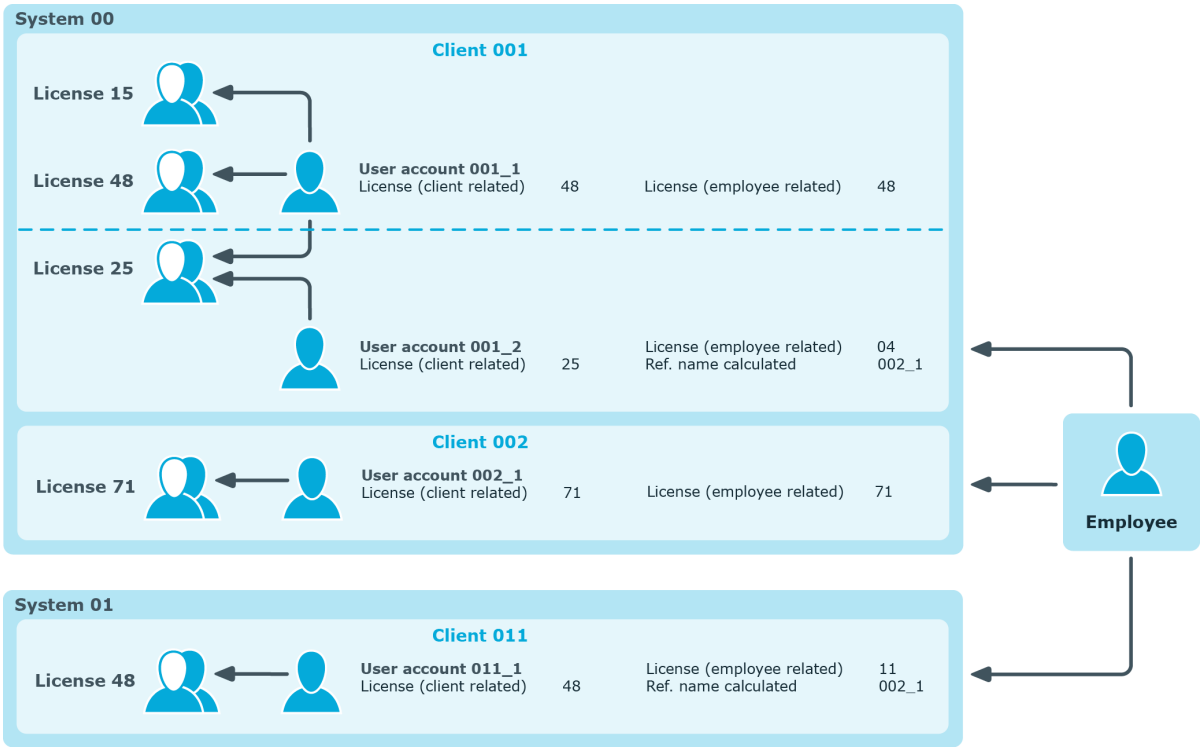
a. The most significant user account is determined from all the identity's user account sin all clients and all systems. The criteria from 1a) and 1b) apply for these user accounts. The license for the most highly rated user account is added to the user account as **Calculated license (identity)**. A reference to the user account calculated with the most significance is entered for all of the identity's other user accounts in **Calculated ref. name**. These user account contain the license "11 (Multi-client/system) or "04 (substitute)".

Table 70: Identity-related license

User accounts	Calculated license (identity)
Most significant user account	Calculated license (client)
Remaining user accounts in clients of the same system as the most significant user account	04 (Deputy manager or supervisor)
Remaining user accounts in other systems besides the most significant user account	11 (Multi-client/system)

b. If a user account is not assigned an identity, the rating calculated under 1) is seen as the most significant and the license entry is added to the user account as **Calculated license (identity)**.

Figure 6: Determining an SAP user account rating



Related topics

- Licenses on page 110
- Disabling license calculation on page 223

Transferring calculated licenses

In order to run system measurement in the SAP R/3 environment, you need to transfer identity 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 the **SAP R/3 > Clients** category.
2. Select the client whose licenses are to be transferred.

3. Select the **Publish calculated licenses** task.

   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 identity 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 identity-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 identity-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 216
- Disabling license calculation on page 223

Disabling license calculation

You can disable calculation of user account ratings for individual SAP client, SAP systems or for all SAP systems managed in One Identity Manager. Licenses calculated for the user accounts are no longer calculated and the active license is not updated. The licenses stored with roles and profiles do not work anymore. Therefore, One Identity Manager does not provide new data for system measurement that is based on currently assigned SAP roles and profiles.

The active license can still be accessed and published in the target system. If active licenses are changed in the target system, the changes are loaded into One Identity Manager by synchronization.

To disable license calculation

- In the Designer, disable the **TargetSystem | SAPR3 | Accounts | CalculateLicence** configuration parameter.

  - OR -

- In SAP, disable the **System measurement enabled** option.

  - OR -

- In the client, disable the **Has user administration**.

Related topics

- Determining an SAP user account rating on page 220
- Transferring calculated licenses on page 222

Reports about SAP objects

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 71: Data quality target system report

Report	Published for	Description
Show overview	User account	This report shows an overview of the user account and the assigned permissions.
Show overview including origin	User account	This report shows an overview of the user account and origin of the assigned permissions.
Show overview including history	User account	This report shows an overview of the user accounts including its history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	group Role Profile Structural profile	This report finds all roles containing identities who have the selected system entitlement.
Show overview	group Role Profile	This report shows an overview of the system entitlement and its assignments.
Show overview including origin	group Role	This report shows an overview of the system entitlement and origin of the assigned user accounts.

Report	Published for	Description
	Profile	
Show overview including history	group Role Profile	This report shows an overview of the system entitlement and including its history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Show entitlement drifts	Client	This report shows all system entitlements that are the result of manual operations in the target system rather than provisioned by One Identity Manager.
Show user accounts overview (incl. history)	Client	This report returns all the user accounts with their permissions including a history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Show user accounts with an above average number of system entitlements	Client	This report contains all user accounts with an above average number of system entitlements.
Show identities with multiple user accounts	Client	This report shows all the identities that have multiple user accounts. The report contains a risk assessment.
Show system entitlements overview (incl. history)	Client	This report shows the system entitlements with the assigned user accounts including a history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	Client system	This report finds all roles containing identities with at least one user account in the selected target system.
Show unused user accounts	Client	This report contains all user accounts, which have not been used in the last few months.
Show orphaned user accounts	Client	This report shows all user accounts to which no identity is assigned.

Table 72: Additional reports for the target system

Report	Description
SAP roles and profiles with rule violations	The report shows all SAP roles and profiles that match SAP functions and thereby violate compliance rules. The report is available if the SAP R/3 Compliance Add-on Module is available.
SAP authorizations, SAP functions, and conflicts	The report presents all rule violations, SAP function and authorization assignments for the selected SAP role/SAP profile including all assignments by child roles/profiles. The report is available if the SAP R/3 Compliance Add-on Module is available.
SAP user account and group administration	This report contains a summary of user account and group distribution in all clients. You can find the report in the **My One Identity Manager > Target system overviews** category.
Data quality summary for SAP user accounts	This report contains different evaluations of user account data quality in all client. You can find the report in the **My One Identity Manager > Data quality analysis** category.

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 identities who own the selected base object. In this case, direct as well as indirect base object assignments are included.

Example: Assignment overview

- If the report is created for a resource, all roles are determined in which there are identities with this resource.
- If the report is created for a group or another system entitlement, all roles are determined in which there are identities with this group or system entitlement.
- If the report is created for a compliance rule, all roles are determined in which there are identities who violate this compliance rule.
- If the report is created for a department, all roles are determined in which identities of the selected department are also members.

- If the report is created for a business role, all roles are determined in which identities 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 **Overview of all assignments** report.
- 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 identities 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 identities 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 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 identities 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 identities for tracking. This creates a new business role to which the identities are assigned.

Figure 7: Toolbar of the Overview of all assignments report.

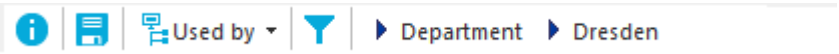


Table 73: Meaning of icons in the report toolbar

Icon	Meaning
	Show the legend with the meaning of the report control elements
	Saves the current report view as a graphic.
	Selects the role class used to generate the report.
	Displays all roles or only the affected roles.

12

Removing a Central User Administration

One Identity Manager supports you in releasing individual clients from a Central User Administration or in completely removing a CUA. After the changeover, individual clients can be managed independently of each other in One Identity Manager. Some tasks can be automated, others must be performed manually afterward. For example, this includes setting up new synchronization projects and removing the CUA distribution model from the SAP R/3 environment.

Recommendations

- Link user accounts to identities

  Before removing a CUA, you must ensure that each user account is linked to an identity. When the CUA is removed, a new user account is created in each client. Therefore, if a user account has access permissions in different clients, multiple user accounts are created. The connection between these user accounts can be established only through the linked identity.

- Create a backup of the One Identity Manager database

  The data conversion cannot be undone. Make sure that there is an up-to-date backup of the One Identity Manager database.

To remove a CUA, first release the individual child systems and check for successful conversion. After all child systems have been detached, you can convert the central system and delete the CUA from the SAP R/3 environment's distribution model.

Detailed information about this topic

- Release child systems on page 230
- Converting the central system on page 231
- Checking for successful conversion on page 233

Related topics

- Central user administration in One Identity Manager on page 136

Release child systems

The child systems can be released individually from the CUA without removing it entirely. Removing a CUA can be done step-by-step and tested. The following steps must be performed for each child system:

a. Release the child system in One Identity Manager from the CUA
b. Set up a new synchronization project and synchronize the client
c. Release child systems from the CUA distribution model of the SAP R/3 environment

To release a child system from the CUA

1. In the Manager, select the **SAP R/3 > Clients** category.
2. In the result list, select the child system you want to release.
3. Select the **Release client from CUA** task and confirm the security prompt with **Yes**.

After checking whether the client can be removed, One Identity Manager converts the data.

- User accounts and their external identifiers are copied from the central system to the child system.
- SAP groups and group assignments to user accounts are copied from the central system to the child system.
- SAP roles and profiles are converted and assigned to the copied user accounts.
- Removes user account access permissions to the child system (purges `SAPUserMandant` table).
- The client assignment to the central system is removed.
- If an account definition is assigned to the client, it is converted. The `SAPUser` table is assigned as a user account table.

To set up synchronization for the released client

1. If the client is hosted in a different SAP system than the central system, then there is a synchronization project for the client. Delete this synchronization project.
2. Create a new synchronization project. For this purpose, use the **SAP R/3 synchronization (base administration)** project template.

   For more information, see Creating a synchronization project for initial synchronization of an SAP client on page 25.

   > TIP: If a suitable synchronization project already exists for an SAP client with an identical schema, then the released client can be assigned to this synchronization project as another base object.
3. Start the synchronization.
4. Check the synchronization result. Fix errors and handle outstanding objects.

To release the child system from the CUA distribution model

- If the synchronization was run without errors, delete the child system from the CUA distribution model in the SAP R/3 environment.

  Only the client assignment to the CUA distribution model is to be removed. For more information, see your SAP R/3 documentation.

Related topics

- Checking for successful conversion on page 233
- Converting the central system on page 231

Converting the central system

As soon as all child systems have been removed from a central user administration, the central system can also be converted. The following steps must be performed:

a. Convert the central system in One Identity Manager
b. Delete user accounts without central system access
c. Delete the CUA from the distribution model of the SAP R/3 environment
d. Set up a new synchronization project and synchronize the client

To convert the central system

1. In the Manager, select the **SAP R/3 > Clients** category.
2. Select the target system in the result list.
3. Select the **Release client from CUA** task and confirm the security prompt with **Yes**.

   After checking whether the client qualifies for conversion, the data is converted in the One Identity Manager database.

   - Converts SAP roles and profiles in the central system.
   - Converts SAP role and profile assignments to user accounts.
   - Removes user account access permissions to the central system (purges `SAPUserMandant` table).
   - Removes the client's central system identifier.
4. Once conversion is complete, it is necessary to decide how to proceed with user accounts that did not have access permissions to the central system within the CUA.

   - If you want to delete these user accounts, click **Yes**.

     Select this option to ensure that only the users who were authorized to access the client before the conversion are granted access. User accounts created by an IT Shop request or by inheritance of a valid account definition remain intact.

     All other user accounts without access permissions are deleted.

- If you want to keep these user accounts, click **No**.

  The user accounts are retained and are thus authorized for access in this client.

5. Decide what to do with user accounts that were created using a valid account definition. If you want to delete these user accounts, remove the account definition assignment to the identities.

   For more information, see Assigning account definitions to identities on page 81.

IMPORTANT: All provisioning processes must be completed before conversion can continue.

Perform the following step before creating a new synchronization project for the client.

To delete the CUA from the distribution model of the SAP R/3 environment

- Once all child systems have been released from the CUA distribution model in the SAP R/3 environment, you can delete the entire CUA from the distribution model.
  - Specify how to proceed with user accounts that did not have access permissions to the central system within CUA.

    If these user accounts have been deleted in One Identity Manager, select the **Additionally Lock Users Locally** option here.

    As a result, the user accounts that were created using an account definition are locked and do not get access permissions to the client.

  For more information, see your SAP R/3 documentation.

To set up synchronization for the client

1. Delete the synchronization project for the central system.
2. Create a new synchronization project. For this purpose, use the **SAP R/3 synchronization (base administration)** project template.
   - On the **Additional settings** page, disable the **Central User Administration (CUA)** option.

   For more information, see Creating a synchronization project for initial synchronization of an SAP client on page 25.

   TIP: If a suitable synchronization project already exists for an SAP client with an identical schema, then the released client can be assigned to this synchronization project as another base object.
3. Start the synchronization.
4. Check the synchronization result. Fix errors and handle outstanding objects.

   User accounts that did not have access permissions for the central system and were created through an account definition are locked.
5. Check locked user accounts.
   a. Unlock all user accounts that should have access to the client.
   b. Remove the account definition from the linked identity of all user accounts to be deleted.

For more information, see Assigning account definitions to identities on page 81.

Related topics

- Checking for successful conversion on page 233
- Release child systems on page 230

Checking for successful conversion

If all child systems have been removed without errors and the central system has been converted without errors, the CUA is removed. The SAP user accounts in all previously involved clients can be managed either separately or through the linked identity.

To check for correct conversion of a child system

1. In the Manager, select the **SAP R/3 > Clients** category.
2. In the result list, select the client of the former child system.
3. Check the following main data
   - **ALE name**: Value deleted.
   - **ALE model name**: Value deleted.
   - **CUA status**: `None`.
   - **CUA central system**: None assigned.
4. Select the **SAP client overview** task.
5. Click the form element for the assigned account definition and check the account definition's main data.
   - **User account table**: `SAPUser`.
   - **Required account definition**: The central system's account definition is assigned.
6. Check if the required account definition is still needed.

   After the removing the CUA, a user account in the central system is no longer a necessary prerequisite for the creation of a user account in the former child system. In this case, the required account definition can be removed.
7. Synchronization is set up and works correctly.

To check for correct conversion of a central system

1. In the Manager, select the **SAP R/3 > Clients** category.
2. In the result list, select the client of the former central system.
3. Check the following main data

- **ALE name**: Empty value.
- **ALE model name**: Value deleted.
- **CUA status**: `None`.

4. Select the **SAP client overview** task.

   No child system is assigned.
5. Synchronization is set up and works correctly.

13

Troubleshooting an SAP R/3 connection

Table accesses not performed correctly

Sometimes the SAP R/3 connector does not perform tables accesses correctly, which causes issues. For example, the leading digits of percentage values with more than five digits (including decimal places) are truncated and replaced by *.

Probable reason

Error in the way the `RFC_READ_TABLE` function module works.

Solution

- Import the current `SAPTRANSPORT_70.ZIP` transport into the SAP R/3 system you want to synchronize.

  As of One Identity Manager version 8.2, an updated BAPI transport `SAPTRANSPORT_70.ZIP` is provided. This uses the `/VIAENET/READTABLE` function module instead of the `RFC_READ_TABLE` SAP module. When it accesses an SAP R/3 system, the SAP R/3 connector checks whether the `/VIAENET/READTABLE` function module exists and uses that.

  If the function module is not available, the connector uses the `RFC_READ_TABLE` SAP module.

The synchronization log records whether the `/VIAENET/READTABLE` function module is used.

Related topics

- Creating a schema extension file on page 48
- Installing the One Identity Manager Business Application Programing Interface on page 18
- Users and authorizations for synchronizing with SAP R/3 on page 15

Appendix A

Configuration parameters for managing an SAP R/3 environment

The following configuration parameters are available in One Identity Manager after the module has been installed.

Table 74: Configuration parameter

Configuration parameters	Description
TargetSystem | SAPR3	SAP is supported. The parameter is a precompiler dependent configuration parameter. Changes to the parameter require recompiling the database. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
TargetSystem | SAPR3 | Accounts	Default values should be used for SAP user accounts.
TargetSystem | SAPR3 | Accounts | CalculateLicence	Parameter for controlling the calculation of SAP system measurement for SAP user accounts.
TargetSystem | SAPR3 | Accounts | CentralSAPAccountGlobalUnique	Specifies how the central SAP user account is mapped. If the configuration parameter is set, the central SAP user account of an identity is formed uniquely in relation to the central user accounts of all identities and the SAP user account names of all permitted SAP systems. If the configuration parameter is not set, the name is only formed with respect to the central SAP user account of all identities.
TargetSystem | SAPR3 | Accounts | Datfm	Specifies the default date format for SAP user accounts.

Configuration parameters	Description
TargetSystem | SAPR3 | Accounts | Dcpfm	Specifies the default decimal point format for SAP user accounts.
TargetSystem | SAPR3 | Accounts | ExtID_Type	Specifies the default type for external identification of SAP user accounts.
TargetSystem | SAPR3 | Accounts | Fax_Group	Specifies the default fax group for SAP user accounts.
TargetSystem | SAPR3 | Accounts | Guiflag	Specifies whether secure communication is permitted for SAP user accounts.
TargetSystem | SAPR3 | Accounts | InitialRandomPassword	Specifies whether a random password is generated when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem | SAPR3 | Accounts | InitialRandomPassword | SendTo	This configuration parameter specifies to which identity the email with the random generated password should be sent (manager cost center-/department/location/business role, identity'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.
TargetSystem | SAPR3 | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Mail template name that is sent to supply users with the login credentials for the user account. The **Identity - new user account created** mail template is used.
TargetSystem | SAPR3 | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Mail template name that is sent to supply users with the initial password. The **Identity - initial password for new user account** mail template is used.
TargetSystem | SAPR3 | Accounts | Langu_p	Specifies default language key for SAP users.
TargetSystem | SAPR3 | Accounts | Langup_iso	Specifies default language (ISO 639).
TargetSystem | SAPR3 | Accounts | MailTemplateDefaultValues	Mail template used to send notifications about whether default IT operating data mapping values are used for automatically creating a user account. The **Identity - new user account with default properties created** mail template is used.
TargetSystem | SAPR3 | Accounts | Spda	Specifies default setting for printer parameter 3 (delete after print).

Configuration parameters	Description
TargetSystem | SAPR3 | Accounts | Spdb	Specifies default setting for printer parameter 3 (print immediately).
TargetSystem | SAPR3 | Accounts | Splg	Specifies the default printer (print parameter 1).
TargetSystem | SAPR3 | Accounts | TargetSystemID	Specifies default target system identification for mapping external users.
TargetSystem | SAPR3 | Accounts | Time_zone	Specifies the default time zone value for the SAP user account's address.
TargetSystem | SAPR3 | Accounts | Tzone	Specifies the default value for the time zone.
TargetSystem | SAPR3 | Accounts | Ustyp	Specifies the default user type for SAP user accounts.
TargetSystem | SAPR3 | AutoCreateDepartment	This configuration parameter specifies whether departments are automatically created when user accounts are modified or synchronized.
TargetSystem | SAPR3 | AutoFillSAPUserMandant	Specifies whether SAP roles and SAP profiles can be inherited by the user accounts in a Central User Administration if the user accounts do not have access permission for the clients that these roles and profile belong to. If the configuration parameter is set, access permission is granted when inheritance is calculated (entry in the `SAPUserMandant` table) and the roles and profiles are assigned to the user accounts. If the configuration parameter is not set, these roles and profiles are not inherited (default).
TargetSystem | SAPR3 | DefaultAddress	Default email address (recipient) for messages about actions in the target system.
TargetSystem | SAPR3 | KeepRedundantProfiles	This configuration parameter regulates behavior for handling single role and profile assignments to users. If the parameter is set, the user's single roles or profiles, which are already part of the user's composite roles, are retained. If the parameter is not set, the user's single roles or profiles, which are already part of the user's composite roles, are removed (default).
TargetSystem | SAPR3 | MaxFullsyncDuration	Specifies the maximum runtime for synchronization.

Configuration parameters	Description
TargetSystem | SAPR3 | PersonAutoDefault	Mode for automatic identity assignment for user accounts added to the database outside synchronization.
TargetSystem | SAPR3 | PersonAutoDisabledAccounts	Specifies whether identities are automatically assigned to disabled user accounts. User accounts are not given an account definition.
TargetSystem | SAPR3 | PersonAutoFullsync	Mode for automatic identity assignment for user accounts that are added to or updated in the database by synchronization.
TargetSystem | SAPR3 | ValidDateHandling	This configuration parameter is for handling validity periods in SAP role and structural profile assignments to SAP user accounts.
TargetSystem | SAPR3 | ValidDateHandling | DoNotUsePWODate	This configuration parameter specifies whether the validity period is taken from the request and copied to the SAP role and structural profile assignments to SAP user accounts. If the configuration parameter is set, the **Valid from** and **Valid until** dates are not copies from the request to the assignments.
TargetSystem | SAPR3 | ValidDateHandling | ReuseInheritedDate	Controls reuse of existing SAP role and structural profile assignments to SAP user accounts. If this configuration parameter is set, existing assignments are reused if the same assignment is created by different means of inheritance and the validity period matches.
TargetSystem | SAPR3 | ValidDateHandling | ReuseInheritedDate | UseTodayForInheritedValidFrom	This configuration parameter specifies whether the **Valid from** data of indirect SAP role and structural profile assignments to SAP user accounts is set to **<today>** or to **1900-01-01**.

Appendix B

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 240
- Project template for the CUA central system on page 241
- Project template for CUA subsystems on page 243

Project template for client without CUA

Use the **SAP R/3 synchronization (base administration)** project template to synchronize clients that are not connected to a central user administration. The project template uses mappings for the following schema types.

Table 75: Mapping SAP R/3 schema types to tables in the One Identity Manager schema.

Schema type in the target system	Table in the One Identity Manager Schema
Company	SAPCompany
GROUP	SAPGrp

Schema type in the target system	Table in the One Identity Manager Schema
LICENSETYPE	SAPLicence
LicenceExtension	SAPLicenceExtension
LoginLanguage	SAPLoginLanguages
CLIENT	SAPMandant
Parameters	SAPParameter
Printer	SAPPrinter
PROFILE	SAPProfile
ProfileInProfile	SAPProfileInSAPProfile
ProfileInRole	SAPProfileInSAPRole
PROFITCENTER	SAPProfitCenter
ROLE	SAPRole
RoleInRole	SAPRoleInSAPRole
STARTMENUE	SAPStartMenu
SAPTSAD3T	SAPTitle
USER	SAPUser
UserComFax	SAPComFax
UserComPhone	SAPComPhone
UserComSMTP	SAPComSMTP
SAPCOMMTYPE	SAPCommType
UserExtId	SAPUserExtId
UserHasParameter	SAPUserHasParameter
UserInGroup	SAPUserInSAPGrp
UserInProfile	SAPUserInSAPProfile
UserInRole	SAPUserInSAPRole

Project template for the CUA central system

Use the **SAP R/3 synchronization (base administration)** project template to synchronize a central user administration central system. The project template uses

mappings for the following schema types.

Table 76: Mapping SAP R/3 schema types to tables in the One Identity Manager schema.

Schema type in the target system	Table in the One Identity Manager Schema
ALE	SAPMandant
CLIENT	SAPMandant
Company	SAPCompany
GROUP	SAPGrp
LICENSETYPE	SAPLicence
LicenceExtension	SAPLicenceExtension
LoginLanguage	SAPLoginLanguages
Parameters	SAPParameter
Printer	SAPPrinter
CUAProfile	SAPProfile
ProfileInProfile	SAPProfileInSAPProfile
ProfileInRole	SAPProfileInSAPRole
PROFITCENTER	SAPProfitCenter
CUARole	SAPRole
RoleInRole	SAPRoleInSAPRole
STARTMENUE	SAPStartMenu
SAPTSAD3T	SAPTitle
USER	SAPUser
UserComFax	SAPComFax
UserComPhone	SAPComPhone
UserComSMTP	SAPComSMTP
UserExtId	SAPUserExtId
UserHasLicense	SAPUserHasLicence
UserHasParameter	SAPUserHasParameter
UserInGroup	SAPUserInSAPGrp
UserInMandant	SAPUserInSAPMandant
UserInCUAProfile	SAPUserInSAPProfile
UserInCUARole	SAPUserInSAPRole

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 project template uses mappings for the following schema types.

Table 77: Mapping SAP R/3 schema types to tables in the One Identity Manager schema.

Schema type in the target system	Table in the One Identity Manager Schema
LICENSETYPE	SAPLicence
LicenceExtension	SAPLicenceExtension
LoginLanguage	SAPLoginLanguages
CLIENT	SAPMandant

Appendix C

Referenced SAP R/3 table 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 have been carried out, apart from the BAPI calls from /VIAENET/.

Table 78: Referenced tables and BAPIs

Tables	BAPI Calls
• ADR2 • ADR3 • ADR6 • ADRP • AGR_1016 • AGR_AGRS • AGR_DEFINE • AGR_USERS • ANLA • ANLZ • AUTHX • CSKS • CSKT • DD02L • DD03L • DD03M • DD04L • DD04T • DD07L	• BAPI_USER_CREATE1 • BAPI_USER_GET_DETAIL • BAPI_USER_CHANGE • BAPI_USER_DELETE • BAPI_USER_LOCK • BAPI_USER_UNLOCK • BAPI_USER_ACTGROUPS_ASSIGN • BAPI_USER_ACTGROUPS_DELETE • BAPI_USER_PROFILES_ASSIGN • BAPI_USER_PROFILES_DELETE • BAPI_USER_LOCACTGROUPS_READ • BAPI_USER_LOCACTGROUPS_DELETE • BAPI_USER_LOCPROFILES_READ • BAPI_USER_LOCPROFILES_DELETE • BAPI_USER_SYSTEM_ASSIGN • SUSR_USER_CHANGE_PASSWORD_RFC • BAPI_USER_LOCPROFILES_ASSIGN • BAPI_USER_LOCACTGROUPS_ASSIGN • RFC_READ_TABLE or /VIAENET/READTABLE

Tables	BAPI Calls
• HRP1000 • HRP1001 • PA0000 • PA0001 • PA0002 • PA0007 • PA0016 • PA0034 • PA0041 • PA0105 • PA0709 • RSECUSERAUTH • RSECTXT • SEC_POLICY_CUST • SEC_POLICY_RT • T000 • T001 • T001P • T002 • T591S • T500P • T548T • T77PR • T77UA • TACT • TACTT • TACTZ • TMENU01 • TMENU01T • TMENU01R • TOBJ • TOBJT • TOBCT	

Tables	BAPI Calls
• TPARA • TSAD3 • TSAD3T • TSAC • TSACT • TSP03 • TSTC • TSTCT • TTREE • TTREET • TUPLT • TUTYP • TUTYPA • TUTYPPL • TUZUS • USGRP_USER • USGRPT • USL04 • USLA04 • USOBHASH • USOBT_C • USOBX_C • USR01 • USR02 • USR05 • USR06 • USR06SYS • USR10 • USR11 • USR12 • USR21 • USREFUS • USREXTID	

Tables	BAPI Calls
• USRSTAMP • USRSYSACTT • USRSYSPRF • USRSYSPRFT • UST04 • UST10C • UST10S • UST12 • USVART • USZBVLNDSC • USZBVLNDRC • USZBVSYS • V_USCOMPA	

Appendix D

Example of a schema extension file

```
<?xml version="1.0" encoding="utf-8" ?>
<SAP>
    <Functions>
        <Function Definition = "USER GET" FunctionName="BAPI_USER_GET_DETAIL" OutStruc-
ture = "" 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 = "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" />
        <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 = "BWPro-
fileAdd" DeleteObjectDefinition = "BWProfileDel" />
        <SAPExtendedSchematype Bem = "simple read only
table" Name = "LicenceExtension" DisplayPattern="%SONDERVERS%" ListObjectsDefinition =
"TUZUS-Table" ReadObjectDefinition ="TUZUS-Table" InsertObjectDefinition = "" WriteOb-
jectDefinition = "" DeleteObjectDefinition = "" ParentType = "SAPSYSTEM" />
        <SAPExtendedSchematype
Bem = "Test" Name = "USERFunctionTable" DisplayPattern="%BNAME% (%MANDT%)" ListOb-
jectsDefinition = "USR05-Table" ReadObjectDefinition ="USER
GET" WriteObjectDefinition = "USER SET" DeleteObjectDefinition = "USER DEL" >
            <Properties>
                <Property Name = "SAPBWP" Description="all BW profiles of the
user" ListFunction="RSECUSERAUTH-
SingleUser" AddFunction="BWProfileAddFkt" DelFunction="BWProfileDelFkt" ReplaceFunction
="" IsMultivalued = "true" />
                <Property Name = "USERPROFILE" Description="all profiles of the
user" ListFunction="USR04-Table" AddFunction="" DelFunction="" ReplaceFunction="USER
```

```
PROFILE SET" IsMultivalued = "true" />
            </Properties>
        </SAPExtendedSchematype>
    </SAPExtendedSchematypes>
</SAP>
```

Detailed information about this topic

- Creating a schema extension file on page 48

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 and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

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

Index

A

account definition 136
- add to IT Shop 85
- assign automatically 73
- assign role 83
- assign to business role 83
- assign to client 88
- assign to identities 84
- assign to system roles 85
- create 72
- delete 88
- for IT Shop 73
- inheritance 73, 77, 81

ALE model name 38
application role 12
application server 9
architecture 9

B

BAPI transport 18, 21
- uninstall 21

base object 43, 63
business role
- assign role 180
- assign to group 180
- assign to product 206
- assign to profile 180

C

calculation schedule
- deactivate 65

category 129
central user administration 136
- solve 229
- user account 155

child system
- access permissions 136
- convert to default client 230
- no synchronization 38

client 127
- category 194
- child system 127
- identity assignment 162
- login data 127
- target system manager 127

communications type 110
company address 109
configuration parameter 236
connection parameter 25
connector schema
- extend 46

convert connection parameter 43
cost center
- assign to group 178
- assign to product 206
- assign to profile 178
- assign to role 178
- SAP R/3 109

country surcharge 110, 216
CUA 136

D

database server 9
department
assign to group 178
assign to product 206
assign to profile 178
assign to role 178
deputy
license data 216
direction of synchronization
direction target system 25, 41
in the Manager 25

E

email address 148
email notification 123
exclusion definition 191
external ID
type 100

F

fax 147

G

group
assign business roles 180
assign cost center 178
assign department 178
assign extended properties 196
assign location 178
assign shelf 186
assign system role 184
assign user account 182
category 172, 194
effective 191
exclusion 191
inheritance 77
IT Shop 172
manage 171
overview 190
risk index 172

I

identity assignment
manual 163
remove 163
search criteria 162
inheritance
category 194
IT operating data
change 80
create mapping rule 78
IT Shop shelf
assign account definition 85

J

Job server
load balancing 64
properties 91

L

license 110
active 216
country surcharge 110
enable calculation 223
rating 110

special version 110
license extension 111
load balancing 64
location
assign to group 178
assign to product 206
assign to profile 178
assign to role 178
login data 123
login language 109

M

main system 136
convert to default client 231
synchronizing 36
manage level
edit 75
inheritance 77
membership
modify provisioning 61
message server 9

N

notification 123

O

object
delete immediately 58
outstanding 58
publish 58
offline mode 67
outstanding object 58

P

parameter
assign system role 104
parameter (SAP R/3) 101
assign 150
assign to business role 103
assign to cost center 102
assign to department 102
assign to location 102
display 101
main data 102
overview form 101
properties 102
parameter value (SAP R/3)
allocate indirect assign 105
change indirect assign 105
delete indirect assign 105
password
initial 123
password policy 112
assign 113
character sets 117
check password 122
conversion script 119-120
default policy 113, 115
display name 115
edit 115
error message 115
excluded list 121
failed logins 116
generate password 122
initial password 116
name components 116
password age 116

password cycle 116
password length 116
password strength 116
predefined 112
test script 119
phone 146
printer 108
product 202
assign business role 206
assign cost center 206
assign department 206
assign extended properties 213
assign group 210
assign identity 207
assign location 206
assign profile 210
assign role 210
assign shelf 208
assign system role 207
conflicting system role 213
deactivate 203
IT Shop 203
manager 203
overview 210
remove from IT Shop 208
risk index 203
share date 203
profile
assign business roles 180
assign cost center 178
assign department 178
assign extended properties 196
assign location 178
assign shelf 186
assign system role 184
assign user account 182
calculated license 219
category 175, 194
effective 191
exclusion 191
IT Shop 175
license 175
manage 171
overview 190
pass down
CUA 190
limit 188
risk index 175
show authorization object 197
project template 240
provisioning
accelerate 64
members list 61

R

report
overview of all assignments 227
revision filter 57
role
assign business roles 180
assign cost center 178
assign department 178
assign extended properties 196
assign location 178
assign shelf 186
assign system role 184
assign user account 183
calculated license 219
category 174, 194
effective 191

exclusion 191
IT Shop 174
license 174
manage 171
only synchronize changes 57
overview 190
pass down
configure 189
CUA 190
limit 188
risk index 174
show authorization object 197
role assignment
validity period 197
router 9

S

SAP product
assign account definition 212
assign parameter 211
assign subscribable reports 212
SAP R/3
troubleshooting 235
SAP user account
assign structural profiles 154
department 165
manage 131
schema
changes 45
shrink 45
update 45
schema type
add additionally 46
security policies 110, 144
security policy attribute 110
server function 94
single object synchronization 63, 66
accelerate 64
special version 110-111, 216
start menu 109
start up configuration 43
subscribable report 212
synchronization
accelerate 57
authorizations 15
base object
create 42
configure 25, 40
connection data 25
connection parameter 25, 40, 42
different clients 42
extended schema 42
limit synchronization object 58
only changes 57
prevent 65
scope 40
start 25
synchronization project
create 25
table access error 235
target system schema 42
variable 40
variable set 42
workflow 25, 41
synchronization analysis report 65
synchronization configuration
customize 40-42
synchronization log 39
synchronization project
create 25

deactivate 65
edit 130
project template 240
synchronization server 9
configure 21
edit 90
install 21
server function 94
synchronization workflow
create 25, 41
synchronize single object 66
system 126
report 225
system connection 25
change 43
enabled variable set 44
system measurement 215
CUA system 156
deputy license 223
determine active license 219
enter active license 156
find rating 220
license extension 156
publish license 222
register active license 218

T

target system
not available 67
target system managers 96
target system synchronization 58
template
IT operating data, modify 80

U

user account
address data 139, 144
administrative user account 133
apply template 80
assign central system 155
assign child system 155
assign extended properties 158
assign group 152
assign identity 132, 160
assign profile 152
assign role 153
calculated license 222
category 139, 194
default user accounts 133
delete 167
deputy 216
deputy license 223
email address 148
external ID 169
fax number 147
fixed value 149
identity 133, 139
license data 216
lock 77, 166-167
lock (SAP R/3) 158
login data 144
manage level 152
measurement data 216
overview form 151
password 123, 144
notification 123
privileged user account 133, 139
productive license 218, 222

rating 220
reference user 144
rename (SAP R/3) 159
retrieve 167
risk index 139
set up 138
SNC name 150
telephone number 146
type 133
user name 139
user account type 99, 144

V

valid from 197
valid until 197
variable set 43
active 44