



## One Identity Manager 9.3

# Administration Guide for Connecting to Oracle E-Business Suite

**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](http://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 Oracle E-Business Suite  
Updated - 06 January 2025, 11:34

For the most recent documents and product information, see [Online product documentation](#).

# Contents

<b>Mapping an Oracle E-Business Suite in One Identity Manager</b> .....	<b>9</b>
Architecture overview .....	9
One Identity Manager users for managing Oracle E-Business Suite .....	10
Configuration parameters .....	11
<b>Synchronizing Oracle E-Business Suite</b> .....	<b>13</b>
Setting up initial synchronization of Oracle E-Business Suite .....	14
Users and permissions for synchronizing with Oracle E-Business Suite .....	15
How to prepare the synchronization user .....	16
Setting up the E-Business Suite synchronization server .....	17
System requirements for the synchronization server .....	17
Installing the One Identity Manager Service .....	18
Creating a synchronization project for initial synchronization of Oracle E-Business Suite .....	21
Information required for setting up a synchronization project .....	21
Setting up an initial synchronization project .....	23
Setting up a synchronization project for identity data .....	27
Setting up a synchronization project for organizational data .....	28
Configuring the synchronization log .....	29
Customizing the synchronization configuration .....	30
Important notes for adjusting existing synchronization projects .....	31
Configuring synchronization in Oracle E-Business Suite .....	31
Configuring synchronization of several Oracle E-Business Suite systems .....	32
Changing system connection settings of Oracle E-Business Suite systems .....	33
Editing connection parameters in the variable set .....	33
Editing target system connection properties .....	35
Updating schemas .....	35
Configuring department synchronization .....	36
Speeding up synchronization with revision filtering .....	37
Using specific statements for database initialization .....	38
Using additional schema types .....	39
Creating a schema extension file .....	41

Object definitions .....	42
Table definitions .....	43
Task definitions .....	46
Symbolic variables in WHERE clauses .....	49
Configuring single object synchronization .....	49
Accelerating provisioning and single object synchronization .....	50
Running synchronization .....	51
Starting synchronization .....	52
Displaying synchronization results .....	53
Deactivating synchronization .....	54
Synchronizing single objects .....	54
Tasks following synchronization .....	55
Post-processing outstanding objects .....	55
Adding custom tables to the target system synchronization .....	57
Troubleshooting .....	57
Ignoring data error in synchronization .....	58
Pausing handling of target system specific processes (Offline mode) .....	59
<b>Managing E-Business Suite user accounts and persons .....</b>	<b>61</b>
Setting up account definitions .....	62
Creating account definitions .....	63
Main data for account definitions .....	63
Creating manage levels .....	65
Main data for manage levels .....	67
Creating mapping rules for IT operating data .....	68
Entering IT operating data .....	69
Modify IT operating data .....	70
Assigning account definitions to identities .....	71
Assigning account definitions to departments, cost centers, and locations .....	72
Assigning account definitions to business roles .....	73
Assigning account definitions to all identities .....	73
Assigning account definitions directly to identities .....	74
Assigning account definitions to system roles .....	74
Adding account definitions in the IT Shop .....	75
Assigning account definitions to target systems .....	77
Deleting account definitions .....	78

Assigning identities automatically to E-Business Suite user accounts .....	80
Editing search criteria for automatic identity assignment .....	82
Finding identities and directly assigning them to user accounts .....	83
Changing the manage level in user accounts .....	84
Assigning account definitions to linked user accounts .....	85
Manually linking identities to E-Business Suite user accounts .....	85
Linking E-Business Suite user accounts with imported identities .....	86
Special features for the deletion of identities .....	88
Supported user account types .....	88
Default user accounts .....	89
Administrative user accounts .....	90
Providing an administrative user account for one identity .....	91
Providing an administrative user account for multiple identities .....	92
Privileged user accounts .....	93
<b>Login credentials .....</b>	<b>95</b>
Password policies for E-Business Suite user accounts .....	95
Predefined password policies .....	96
Using password policies .....	97
Editing password policies .....	98
General main data of password policies .....	99
Policy settings .....	99
Character classes for passwords .....	101
Custom scripts for password requirements .....	102
Checking passwords with a script .....	103
Generating passwords with a script .....	104
Editing the excluded list for passwords .....	105
Checking passwords .....	106
Testing the generation of passwords .....	106
Initial password for new E-Business Suite user accounts .....	106
Email notifications about login data .....	107
<b>Managing entitlement assignments .....</b>	<b>109</b>
Assigning E-Business Suite entitlements to user accounts in One Identity Manager ...	110
Prerequisites for indirect assignment of E-Business Suite entitlements to E- Business Suite user accounts .....	111

Assigning E-Business Suite entitlements to departments, cost centers, and locations .....	112
Assigning E-Business Suite entitlements to business roles .....	113
Adding E-Business Suite entitlements to system roles .....	114
Adding E-Business Suite entitlements to the IT Shop .....	115
Assigning E-Business Suite user accounts directly to an entitlement .....	117
Assigning E-Business Suite entitlements directly to a user account .....	118
Validity period of permission assignments .....	120
Effectiveness of entitlement assignments .....	122
Inheritance of E-Business Suite entitlements based on categories .....	125
Invalid entitlement assignments .....	127
Overview of all assignments .....	128
<b>Mapping E-Business Suite objects in One Identity Manager .....</b>	<b>130</b>
E-Business Suite systems .....	130
General main data of E-Business Suite systems .....	130
Defining categories for the inheritance of E-Business Suite entitlements .....	132
Editing the synchronization project for an E-Business Suite system .....	132
E-Business Suite user accounts .....	133
Entering main data of E-Business Suite user accounts .....	134
General main data of E-Business Suite user accounts .....	134
Login data for E-Business Suite user accounts .....	138
Additional tasks for managing E-Business Suite user accounts .....	139
Displaying the E-Business Suite user account overview .....	140
Assigning extended properties to E-Business Suite user accounts .....	140
Disabling E-Business Suite user accounts .....	140
Deleting E-Business Suite user accounts .....	142
E-Business Suite permissions .....	142
Entering main data of E-Business Suite entitlements .....	143
General main data of an E-Business Suite entitlement .....	143
Additional tasks for managing E-Business Suite entitlements .....	144
Displaying E-Business Suite entitlement overviews .....	145
Assigning extended properties to E-Business Suite entitlements .....	145
E-Business Suite applications .....	146
E-Business Suite menus .....	146
E-Business Suite data groups .....	147

E-Business Suite data group units .....	148
E-Business Suite request groups .....	148
E-Business Suite security groups .....	149
E-Business Suite attributes .....	149
E-Business Suite responsibilities .....	150
Displaying main data of E-Business Suite responsibilities .....	151
General main data of E-Business Suite responsibilities .....	151
HR people .....	152
Suppliers and contacts .....	153
Parties .....	154
Locations .....	156
Departments .....	156
Reports about E-Business Suite objects .....	157
<b>Handling of E-Business Suite objects in the Web Portal .....</b>	<b>160</b>
<b>Basic configuration data .....</b>	<b>162</b>
Job server for E-Business Suite-specific process handling .....	163
Editing E-Business Suite Job servers .....	163
General main data of Job servers .....	164
Specifying server functions .....	167
Target system managers .....	168
<b>Appendix: Configuration parameters for managing Oracle E-Business Suite .....</b>	<b>171</b>
<b>Appendix: Permissions required for synchronizing with Oracle E-Business Suite .....</b>	<b>175</b>
<b>Appendix: Default project templates for synchronizing an Oracle E-Business Suite .....</b>	<b>178</b>
Project template for user accounts and entitlements .....	178
Project template for HR data .....	179
Project template for CRM data .....	180
Project template for OIM data .....	180
<b>Appendix: Editing system objects .....</b>	<b>181</b>
<b>Appendix: Example of a schema extension file .....</b>	<b>183</b>
<b>About us .....</b>	<b>187</b>

Contacting us .....	187
Technical support resources .....	187
<b>Index .....</b>	<b>188</b>

---

# Mapping an Oracle E-Business Suite in One Identity Manager

One Identity Manager offers simplified user administration for Oracle E-Business Suite. One Identity Manager concentrates on setting up and editing user accounts as well as providing the required permissions. For this, applications, responsibilities, data groups and data group units, security groups, process groups, menus, and attributes are mapped in One Identity Manager.

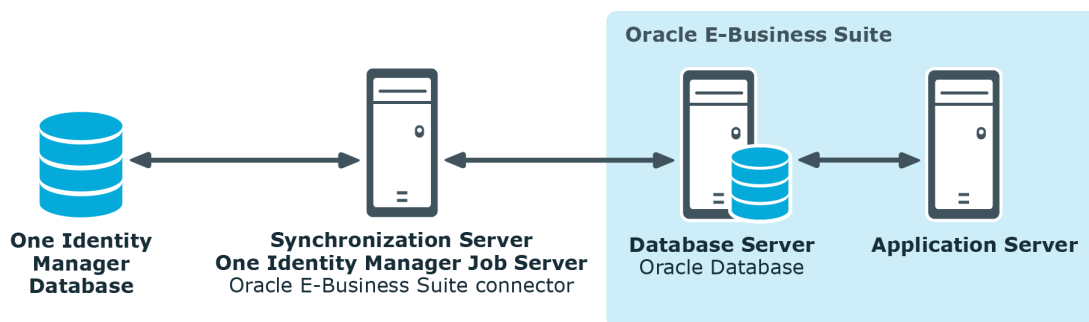
One Identity Manager provides company identities with the necessary user accounts. There are different ways for you to connect identities to their user accounts. You can also manage user accounts independently of identities and thus set up administrator user accounts.

In addition, data can be imported from the Human Resources module (identity data and locations) and organizational data (suppliers, customers, other parties) can also be imported. The imported persons can be provided with all required permissions in the E-Business Suite by their E-Business Suite user accounts. Default One Identity Manager functions, such as the IT Shop or Identity Audit, can be used for these people.

## Architecture overview

To access Oracle E-Business Suite data, the Oracle E-Business Suite connector is installed on a synchronization server. The Oracle E-Business Suite connector establishes communication with the Oracle E-Business Suite to be synchronized. The synchronization server ensures data is synchronized between the One Identity Manager database and Oracle Database.

**Figure 1: Architecture for synchronization**



## One Identity Manager users for managing Oracle E-Business Suite

The following users are used for setting up and administration of E-Business Suite.

**Table 1: Users**

Users	Tasks
Target system administrators	<p>Target system administrators must be assigned to the <b>Target systems   Administrators</b> application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> <li>• Administer application roles for individual target system types.</li> <li>• Specify the target system manager.</li> <li>• Set up other application roles for target system managers if required.</li> <li>• Specify which application roles for target system managers are mutually exclusive.</li> <li>• Authorize other identities to be target system administrators.</li> <li>• Do not assume any administrative tasks within the target system.</li> </ul>
Target system managers	<p>Target system managers must be assigned to the <b>Target systems   Oracle E-Business Suite</b> or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> <li>• Assume administrative tasks for the target system.</li> </ul>

Users	Tasks
One Identity Manager administrators	<ul style="list-style-type: none"> <li>• Create, change, or delete target system objects.</li> <li>• Edit password policies for the target system.</li> <li>• Prepare entitlements to add to the IT Shop.</li> <li>• Can add identities that do not have the <b>Primary identity</b> identity type.</li> <li>• Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.</li> <li>• Edit the synchronization's target system types and outstanding objects.</li> <li>• Authorize other identities within their area of responsibility as target system managers and create child application roles if required.</li> </ul> <p>One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p> <p>One Identity Manager administrators:</p> <ul style="list-style-type: none"> <li>• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required.</li> <li>• Create system users and permissions groups for non role-based login to administration tools in the Designer as required.</li> <li>• Enable or disable additional configuration parameters in the Designer as required.</li> <li>• Create custom processes in the Designer as required.</li> <li>• Create and configure schedules as required.</li> <li>• Create and configure password policies as required.</li> </ul>

## Configuration parameters

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 Oracle E-Business Suite](#) on page 171.

# Synchronizing Oracle E-Business Suite

One Identity Manager supports synchronization with Oracle E-Business Suite 12.1, 12.2, and 12.2.10. The One Identity Manager Service is responsible for synchronizing data between the One Identity Manager database and Oracle E-Business Suite.

This sections explains how to:

- Set up synchronization to import initial data from Oracle E-Business Suite to the One Identity Manager database.
- Adjust a synchronization configuration, for example, to synchronize different E-Business Suite systems with the same synchronization project.
- Start and deactivate the synchronization.
- Analyze synchronization results.

**TIP:** Before you set up synchronization with Oracle E-Business Suite, familiarize yourself with the Synchronization Editor. For more information about this tool, see the *One Identity Manager Target System Synchronization Reference Guide*.

## Detailed information about this topic

- [Setting up initial synchronization of Oracle E-Business Suite](#) on page 14
- [Customizing the synchronization configuration](#) on page 30
- [Running synchronization](#) on page 51
- [Troubleshooting](#) on page 57
- [Editing system objects](#) on page 181

## Related topics

- [Architecture overview](#) on page 9

# Setting up initial synchronization of Oracle E-Business Suite

The Synchronization Editor provides several project templates with which Oracle E-Business Suite user accounts and entitlements can be selected from either organizational data or data from the Human Resource Module for setting up synchronization. You use these project templates to create synchronization projects with which you import the data from an Oracle E-Business Suite into your One Identity Manager database. In addition, processes are created that are required to provision changes to target system objects from the One Identity Manager database into the target system.

## **To create a synchronization configuration for the initial synchronization of an Oracle E-Business Suite:**

1. Prepare a user account with sufficient permissions for synchronizing in Oracle E-Business Suite.
2. One Identity Manager components for managing Oracle E-Business Suite environments are available if the **TargetSystem | EBS** 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.
3. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.
4. Create a synchronization project with the Synchronization Editor.

## **Detailed information about this topic**

- [Users and permissions for synchronizing with Oracle E-Business Suite](#) on page 15
- [System requirements for the synchronization server](#) on page 17
- [Creating a synchronization project for initial synchronization of Oracle E-Business Suite](#) on page 21
- [Configuration parameters for managing Oracle E-Business Suite](#) on page 171
- [Default project templates for synchronizing an Oracle E-Business Suite](#) on page 178

# Users and permissions for synchronizing with Oracle E-Business Suite

The following users play a role in synchronizing One Identity Manager with Oracle E-Business Suite.

**Table 2: Users for synchronization**

User	Permissions
User for accessing the target system (synchronization user)	<p>You must provide a user account with the minimum permissions required for full synchronization of Oracle E-Business Suite objects with the supplied One Identity Manager default configuration. For more information, see <a href="#">How to prepare the synchronization user</a> on page 16 and <a href="#">Permissions required for synchronizing with Oracle E-Business Suite</a> on page 175.</p>
One Identity Manager Service user account	<p>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).</p> <p>The user account must belong to the <b>Domain users</b> group.</p> <p>The user account must have the <b>Login as a service</b> extended user permissions.</p> <p>The user account requires permissions for the internal web service.</p> <p><b>NOTE:</b> If the One Identity Manager Service runs under the network service (<b>NT Authority\NetworkService</b>), you can grant permissions for the internal web service with the following command line call:</p> <pre>netsh http add urlacl url=http://&lt;IP address&gt;:&lt;port number&gt;/ user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager.</p> <p>In the default installation, One Identity Manager is installed under:</p> <ul style="list-style-type: none"><li>• %ProgramFiles(x86)%\One Identity (on 32-bit operating systems)</li><li>• %ProgramFiles%\One Identity (on 64-bit operating systems)</li></ul>

User	Permissions
User for accessing the One Identity Manager database	The <b>Synchronization</b> default system user is provided to run synchronization using an application server.

## How to prepare the synchronization user

You have three ways of providing a synchronization user with all the permissions required for accessing the Oracle E-Business Suite.

- Scenario 1: Use the **APPS** user as the synchronization user.
- Scenario 2: Load the wrapper package supplied into the APPS schema and add the synchronization user using the script provided.
- Scenario 3: Add a synchronization user who has a minimum of all the permissions listed.

In Oracle E-Business Suite version 12.2, the calling permissions of standard packages have been changed (from `CURRENT_USER AUTHID` to `DEFINER AUTHID`). To be able to run operations for user accounts in the target system, you now require the user **APPS**. Use Scenario 1 or 2, in this case, to provide the synchronization user. If you are working with Oracle E-Business Suite 12.1, you can also use scenario 3.

### Scenario 1:

To ensure that the Oracle E-Business Suite can run connector operations for user accounts in the target system, use the **APPS** user as the synchronization user.

### Scenario 2:

If you cannot use the **APPS** user as the synchronization user directly, create a synchronization user with the required minimum permissions. Use the script supplied and the wrapper package to do this. You will find these files on the One Identity Manager installation medium in the `Modules\EBS\dvd\AddOn\SDK` directory.

#### *To add the synchronization user*

1. Add the `FND_USER_wrapper.sql` wrapper package to the APPS schema of your Oracle Database.
2. Add the synchronization user with minimum permissions. Use the script `CreateSyncUser.sql` for this.

Take note of the comment in the script to replace the `&&username` and `&&password` variables.

This script creates a user with the required permissions. The wrapper ensures that the user also obtains the implicit permissions for the package `apps.fnd_user_pkg`.

### Scenario 3:

If you cannot use either scenario 1 or scenario 2, create a synchronization user with all required permissions.

**IMPORTANT:** The synchronization user requires:

- All the permissions listed and also
- All **implicit** permissions for the package apps.fnd\_user\_pkg

#### Detailed information about this topic

- [Permissions required for synchronizing with Oracle E-Business Suite](#) on page 175

## Setting up the E-Business Suite 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.

The One Identity Manager Service with the Oracle E-Business Suite connector must be installed on the synchronization server.

#### Detailed information about this topic

- [System requirements for the synchronization server](#) on page 17
- [Installing the One Identity Manager Service](#) on page 18

## System requirements for the synchronization server

To set up synchronization with Oracle E-Business Suite, 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.

The synchronization server requires a good network connection to the Oracle E-Business Suite's database server.

## Installing the One Identity Manager Service

The One Identity Manager Service with the Oracle E-Business Suite connector must be installed on the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager.

**Table 3: Properties of the Job server**

Property	Value
Server function	Oracle E-Business Suite connector
Machine role	Server   Job Server   Oracle E-Business Suite

**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 **E-Business Suite**.
5. On the **Server functions** page, select **Oracle E-Business Suite 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 Oracle E-Business Suite

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and Oracle E-Business Suite. The following describes the steps for initial configuration of a synchronization project for user accounts and permissions. For more information about setting up synchronization, see the *One Identity Manager Target System Synchronization Reference Guide*.

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.

### Information required for setting up a synchronization project

Have the following information available for setting up a synchronization project.

**Table 4: Information required for setting up a synchronization project**

Data	Explanation
User account and password	User account and password used by the Oracle E-Business Suite connector to log in to the Oracle Database database. Make a user account available with sufficient permissions.  For more information, see <a href="#">How to prepare the synchronization user</a> on page 16.
Data source	<ul style="list-style-type: none"><li>• Oracle Database connection parameter (Connect Descriptor) in the following syntax: <code>(DESCRIPTION=(ADDRESS=(protocol_address_information)) (CONNECT_DATA=(SERVICE_NAME=service_</code></li></ul>

Data	Explanation
	<p>name)))</p> <p>- OR -</p> <ul style="list-style-type: none"> <li>• TNS alias name from the TNSNames.ora file.</li> </ul>
Synchronization server for Oracle E-Business Suite	<p>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.</p> <p>For more information, see <a href="#">Setting up the E-Business Suite synchronization server</a> on page 17.</p>
One Identity Manager database connection data	<ul style="list-style-type: none"> <li>• Database server</li> <li>• Database name</li> <li>• SQL login and password</li> <li>• Specifies whether integrated Windows authentication is used</li> </ul> <p>Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</p>
Remote connection server	<p>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.</p> <p>Remote connection server configuration:</p> <ul style="list-style-type: none"> <li>• One Identity Manager Service is started</li> <li>• <b>RemoteConnectPlugin</b> is installed and an authentication method is set up</li> <li>• Oracle E-Business Suite connector is installed</li> </ul> <p>The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.</p> <p>For more detailed information about setting up a remote connection, see the <i>One Identity Manager Target System Synchronization Reference Guide</i>.</p>

## Setting up an initial synchronization project

**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.

**NOTE:** If a synchronization project is set up for a target system that already exists in the One Identity Manager database, ensure that the same server and the same unique name for the DN are given as in the existing synchronization project.

- When you set up the synchronization project, use an existing system connection with the necessary configuration.  
- OR -
- In the Manager, check the defined name and the display name of the E-Business Suite system you are creating the synchronization for. The following values must match:
  - Display name: **Oracle Finance on <server>**
  - Distinguished name: **O=ORA system,DC=<unique name for the DN>**

### **To set up an initial synchronization project for Oracle E-Business Suite**

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 Oracle E-Business Suite** 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. On the **Database connection** page, enter the connection parameters required by the Oracle E-Business Suite connector to log in to the Oracle Database.

**Table 5: Login credentials for connection to Oracle E-Business Suite**

Property	Description
User	User name used by the connector to log in to the Oracle Database.
Password	Password for logging in to the Oracle Database.
Data source	<ul style="list-style-type: none"><li>• Oracle Database connection parameter (Connect Descriptor) in the following syntax: <pre>(DESCRIPTION=(ADDRESS=(protocol_address_information)) (CONNECT_DATA=(SERVICE_NAME=service_name)))</pre> - OR -</li><li>• TNS alias name from the TNSNames.ora file.</li></ul>

The connection to the Oracle Database is tested the moment you click **Next**.

6. On the **Connection Configuration** page, configure more default parameters for the connection.

**Table 6: Connection configuration**

Property	Description
Language selection	Languages used to load captions from the database.
Unique name for the DN.	Part of name used to generate a distinguished name for all objects in the system. Leave this field empty to use the database server's server name.  This name should not be changed after the initial synchronization.
Read-only	Specifies whether the Oracle E-Business Suite connector only has read access to the target system.
Package to access users	The name of the wrapper package or user package to be used for adding and modifying user accounts and permissions.  Syntax: <owner>.<PackageName>  The following input required, depending on which scenario was used to set up the synchronization user. <ul style="list-style-type: none"> <li>• User <b>APPS</b> (scenario 1): no input required. Default is APPS.FND_User_PKG.</li> <li>• Wrapper (scenario 2): name of the wrapper package. Default is APPS.FND_USER_WRAPPER.</li> <li>• Otherwise (scenario 3): name of the user package. Default is APPS.FND_User_PKG.</li> </ul>

7. On the **Display Name** page, enter a unique display name for the connection configuration.

You can use the display names to differentiate between the connection configurations of different Oracle E-Business Suite connections in the Synchronization Editor. Display names cannot be changed later.

8. On the last page of the system connection wizard, you can save the connection data.
  - Set the **Save connection locally** option to save the connection data. This can be reused when you set up other synchronization projects.
  - Click **Finish**, to end the system connection wizard and return to the project wizard.
9. 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.


10. 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.

11. On the **Select project template** page, select **Oracle E-Business Suite Synchronization**.

**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.

12. 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.

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

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.

## Related topics

- [Configuring the synchronization log](#) on page 29
- [Customizing the synchronization configuration](#) on page 30
- [Project template for user accounts and entitlements](#) on page 178
- [Setting up a synchronization project for identity data](#) on page 27
- [Setting up a synchronization project for organizational data](#) on page 28

## Setting up a synchronization project for identity data

To synchronize data from the Human Resources module of Oracle E-Business Suite, you create a separate synchronization project. A separate project template is provided for this.

**NOTE:** If a synchronization project is set up for a target system that already exists in the One Identity Manager database, ensure that the same server and the same unique name for the DN are given as in the existing synchronization project.

- When you set up the synchronization project, use an existing system connection with the necessary configuration.  
- OR -
- In the Manager, check the defined name and the display name of the E-Business Suite system you are creating the synchronization for. The following values must match:
  - Display name: **Oracle Finance on <server>**
  - Distinguished name: **O=ORA system,DC=<unique name for the DN>**

### ***To set up a synchronization project for identity data:***

- Set up an initial synchronization project. The following special feature applies:  
In the project wizard, on the **Select project template** page, select the **Oracle E-Business Suite HR data** project template.

## Detailed information about this topic

- [Setting up an initial synchronization project](#) on page 23
- [Project template for HR data](#) on page 179

## Related topics

- [Configuring department synchronization](#) on page 36

# Setting up a synchronization project for organizational data

For the synchronization of organizational data such as supplier contact data or parties, you create separate synchronization projects. Separate project templates are provided for this.

**NOTE:** If both synchronization projects are set up on a One Identity Manager database, objects may exist in duplicate after the synchronization.

Create only one of the two synchronization projects for each One Identity Manager database.

**NOTE:** If a synchronization project is set up for a target system that already exists in the One Identity Manager database, ensure that the same server and the same unique name for the DN are given as in the existing synchronization project.

- When you set up the synchronization project, use an existing system connection with the necessary configuration.  
- OR -
- In the Manager, check the defined name and the display name of the E-Business Suite system you are creating the synchronization for. The following values must match:
  - Display name: **Oracle Finance on <server>**
  - Distinguished name: **O=ORA system,DC=<unique name for the DN>**

### ***To set up a synchronization project for supplier contact data***

- Set up an initial synchronization project. The following special feature applies:  
In the project wizard, on the **Select project template** page, select the **Oracle E-Business Suite CRM data** project template.

### ***To set up a synchronization project for party data***

- Set up an initial synchronization project. The following special feature applies:  
In the project wizard, on the **Select project template** page, select the **Oracle E-Business Suite OIM data** project template.

## Detailed information about this topic

- [Setting up an initial synchronization project](#) on page 23
- [Project template for CRM data](#) on page 180
- [Project template for OIM data](#) on page 180

# Configuring the synchronization log

All the information, tips, warnings, and errors that occur during synchronization are recorded in the synchronization log. You can configure the type of information to record separately for each system connection and synchronization workflow.

## ***To configure the content of the synchronization log for a system connection***

1. To configure the synchronization log for target system connection, in the Synchronization Editor, select the **Configuration > Target system** category.

- OR -

To configure the synchronization log for the database connection, in the Synchronization Editor, select the **Configuration > One Identity Manager connection** category.

2. In the **General** section, click **Setup**.
3. In the **Synchronization log** section, set **Create synchronization log**.
4. 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.

5. Click **OK**.

## ***To configure the content of the synchronization log for a synchronization workflow***

1. In the Synchronization Editor, select the **Workflows** category.
2. Select a workflow in the navigation view.
3. In the **General** section, click **Edit**.
4. Select the **Synchronization log** tab.
5. 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.

6. Click **OK**.

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.

## **Related topics**

- [Displaying synchronization results](#) on page 53

# Customizing the synchronization configuration

Having used the Synchronization Editor to set up a synchronization project for initial synchronization of an E-Business Suite system, you can use the synchronization project to load Oracle E-Business Suite objects into the One Identity Manager database. If you manage user accounts and their authorizations with One Identity Manager, changes are provisioned in the Oracle E-Business Suite.

You must customize the synchronization configuration in order to compare the database with the Oracle E-Business Suite regularly 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 Oracle E-Business Suite objects and One Identity Manager database objects are included in the 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 E-Business Suite systems. Store a connection parameter as a variable for logging in to the respective system.
- 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.
- To synchronize additional schema properties, update the schema in the synchronization project. Include the schema extensions in the mapping.
- To define additional instructions for initializing the database connection, edit the target system connection.
- Add your own schema types if you want to synchronize data, which does not have schema types in the connector schema. Include the schema extensions in the mapping.

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

## Detailed information about this topic

- [Configuring synchronization in Oracle E-Business Suite](#) on page 31
- [Configuring synchronization of several Oracle E-Business Suite systems](#) on page 32
- [Updating schemas](#) on page 35

- [Using specific statements for database initialization](#) on page 38
- [Using additional schema types](#) on page 39
- [Changing system connection settings of Oracle E-Business Suite systems](#) on page 33

## Important notes for adjusting existing synchronization projects

If you want to change the configuration of existing synchronization projects, check the possible effects of these changes on the data that has already been synchronized. Note the following information in particular.

### Notes for the synchronization of E-Business Suite identity data

If you change the mappings for synchronization of identity data for a specific company, check whether you also need to change which columns are locked in the Person or Locality table. To lock additional columns for editing in One Identity Manager, define custom scripts (OnLoaded) in the Person or Locality table.

For more information about table scripts, see the *One Identity Manager Configuration Guide*.

### Changing the connection parameters to Oracle E-Business Suite

The connection parameters to the target system can be subsequently changed by the system connection wizard.

The unique name of the DN is used to generate a unique defined name for all objects in the system. If this name is changed after the initial synchronization, the objects will no longer be uniquely identifiable in the next synchronization. This means that all objects will be created again in the One Identity Manager database.

The unique name for the DN should not be changed after the initial synchronization.

If the unique name for the DN must be changed before the initial synchronization, this change must also be transferred to the variable CP\_EBSSystemDN. This variable is used in the filter condition for the scope.

For more information about adjusting the connection parameters and editing variables, see *One Identity Manager Target System Synchronization Reference Guide*.

## Configuring synchronization in Oracle E-Business Suite

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**.

**NOTE:** Only synchronization projects created with the **Oracle E-Business Suite Synchronization** project template contain a provisioning workflow

### ***To create a synchronization configuration for synchronizing Oracle E-Business Suite***

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 several Oracle E-Business Suite systems](#) on page 32

## **Configuring synchronization of several Oracle E-Business Suite systems**

In some circumstances, you are use a synchronization project to synchronize multiple E-Business Suite systems.

### **Prerequisites**

- The target system schema of the E-Business Suite systems are identical.
- All virtual schema properties used in the mapping must exist in the extended schema of the E-Business Suite systems.
- The connection parameters to the target system are defined as variables.

### ***To customize a synchronization project for synchronizing another system***

1. Supply a user in the other system with sufficient permissions for accessing the Oracle E-Business Suite.
2. In the Synchronization Editor, open the synchronization project.

3. Create a new base object for the other system.
  - Use the wizard to attach a base object.
  - In the wizard, select the Oracle E-Business Suite 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

- [Configuring synchronization in Oracle E-Business Suite](#) on page 31

## Changing system connection settings of Oracle E-Business Suite systems

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 33
- [Editing target system connection properties](#) on page 35

## 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 your 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 systems.

### **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 35

## 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 33

## 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.

## **Configuring department synchronization**

To synchronize departments and department memberships, data from the schema types `HROrganization` and `HRPersonInOrganization` is loaded. You must filter required objects to synchronize this data, otherwise performance may be seriously affected if all departments are being synchronized.

If you use default mapping for these schema types, you can select the required departments from the organization hierarchy. To do this, edit the synchronization project's scope and create the hierarchy filter.

Departments can also be differentiated from other organization by their type. Since you can customize these types in Oracle E-Business Suite, departments are not filtered by type in the default maps. To filter departments by type, define your own schema classes.

If you use custom mapping for synchronizing departments, define the filter beforehand in the schema class. In addition, you can use hierarchy filters to limit further the number of synchronization objects.

## Related topics

- [Setting up a synchronization project for identity data](#) on page 27

# 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.

Oracle E-Business Suite supports revision filtering. The E-Business Suite objects' date of last change is used as a revision counter. Each synchronization saves the last date it 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 E-Business Suite 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.

Optimized revision filtering is supported because objects are not deleted in the target system by synchronization and Oracle E-Business Suite makes it possible to find out about the last change to a schema type. If the objects of a schema type were neither added nor changed, the synchronization step can be skipped. Objects must not be loaded for comparison. The Oracle E-Business Suite connector provides all the relevant information.

## To use optimized revision filtering

- In the Designer, set the **Common | TableRevision** configuration parameter.

Now each time a table changes, the table's revision date updates. This information is stored in the QBMTABLERevision table, RevisionDate column. In this way, One Identity Manager identifies whether a table object has been added, changed, or deleted.

Synchronization with revision filtering compares a table's revision date and the schema type's change information against the revision saved in the One Identity Manager

database. If the revision date is older, no objects have been changed in this table since the previous synchronization. If the change information of the schema type is also older, no objects in this schema type have been changed since the previous synchronization. Therefore, synchronization does not carry out this step for the affected table. If the revision date or change information is newer, synchronization does carry out this step and the changed objects are determined as described above.

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.

**NOTE:** If the **Common | TableRevision** is not set, all revision data in the `QBMTTableRevision` table is deleted.

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

## Using specific statements for database initialization

You can make various additional settings on the target system connection, if required due to the configuration of the target system. For example, the default language and time formatting can be overwritten by an SQL statement that is run every time a connection is established.

### **To use additional statements for database initialization:**

1. In the Synchronization Editor, open the synchronization project.
2. Enable expert mode.
3. Edit the target system connection.
  - a. Select the **Configuration > Target system** category.
  - b. Click **Edit connection**.

This starts the system connection wizard.

- c. Select **Database connection startup sequence** page and enter the SQL statements to be run every time a connection is established.

**NOTE:** Only single instructions are supported. In a multi-line statement, each line is processed individually.

#### Example of a multi-line statement

```
alter session set nls_date_format = 'DD-MON-YYYY HH24:MI:SS'  
alter session set nls_language = 'AMERICAN'
```

- d. Click **Test**.
  - e. End the system connection wizard.  
This updates the connection parameters.
4. Save the changes.

If you are running Synchronization Editor in expert mode, SQL statements can be entered when a synchronization project is set up.

## Using additional 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 41.
3. Open the synchronization project in the Synchronization Editor.
4. Enable expert mode.
5. Select the **Configuration > Target system** category.
6. Click **Edit connection**.  
This starts the system connection wizard.
7. Verify the data.
8. Enter the path to the schema extension file on the **Schema extensions (manually)** page.
  - a. To check the schema extensions file for logical errors, click **Test file**.  
All defined schema types are listed.
  - b. Click **Next**.
9. Click **Finish** to end the system connection wizard.
10. Select the view **General** and click **Update schema**.
11. Confirm the security prompt with **Yes**.  
The schema types, including your new schema types, are loaded.
12. 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.
13. 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*.
14. 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*.
15. Save the changes.
16. Run a consistency check.
17. Activate the synchronization project.

### **To remove the schema part of the schema extension file from the connector schema**

1. Delete all mappings and synchronization steps that were created for the additional schema types.
2. Edit the target system connection using the system connection wizard.
  - On the **Expert schema settings** page, click **Clear existing**.
3. Update the schema.
4. Save the changes.
5. Run a consistency check.
6. 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 for the new schema types. Schema types defined here are always added to the existing schema. If a new schema type has the same name as an already existing schema type, the extension is ignored.

You can only specify one schema extension file. This must contains all required extensions. If a schema extension file is added to a connection configuration that already contains a schema extension file, the previous definition is overwritten.

The schema extension file defines schema types as objects, and therefore corresponds to the basic structure of a list of object definitions. An object definition contains the definition of a schema type. A file can contain any number of object definitions.

### **Schema extension file structure**

```
<?xml version="1.0" encoding="utf-8" ?>
<EBSF12>
  <ObjectNames>
    <Object>
      ...
    </Object>
  </ObjectNames>
</EBSF12>
```

### **Detailed information about this topic**

- [Object definitions](#) on page 42
- [Table definitions](#) on page 43

- [Task definitions](#) on page 46
- [Example of a schema extension file](#) on page 183

## Object definitions

The object definitions are used for the formal description of which sources, key values, and conditions are used for the selection of data objects of a schema type. This formal description is evaluated by the Oracle E-Business Suite connector, which uses them to generate SQL statements for the database query. Because data for an object of a schema type can be determined from multiple tables, always use table and column names in the full notation <schema name>.<table name>.<column name>.

Example: AK.AK\_ATTRIBUTES\_TL.ATTRIBUTE\_CODE

**Table 7: Attributes of an object definition**

Attribute	Description
SchemaName	Freely selected name of the schema type to be defined. The objects of this type are displayed in the extended schema under this name.
ParentSchemaName	Reference to an additional schema type on a higher hierarchy level. Example: Application is ParentSchemaName of Attribute
DisplayPattern	Definition of a display pattern for displaying objects in the Synchronization Editor (for example, in the target system browser or when defining schema classes).
IsReadOnly	Specifies whether the objects of this schema type can be read-only. The default value is <b>false</b> .
AddRootDN	Specifies whether the unique name for the DN should be added to the defined name of all objects of this schema type. The default value is <b>true</b> .
UseDistinct	Specifies whether duplicate entries are prevented through the use of the <b>Distinct</b> function. The default value is <b>false</b> .

### Example

```
<Object SchemaName="ORA-Attribute" ParentSchemaName="ORA-Application"
DisplayPattern="%AK.AK_ATTRIBUTES_TL.ATTRIBUTE_CODE%" IsReadOnly="true"
UseDistinct="false" >
```

## Object key definition

The object keys define all columns that are required to select only one object of the schema type. <Key> tags are used to define the key columns. The <ObjectKey> tag can contain any number of <Key> tags. This enables the components of the unique key to be declared for all elements of a schema type and the columns to be named that are required for the identification of an individual object of this schema type. The correct specification of all key columns is important both for the selection of the individual objects, and for possible Join operations.

**Table 8: Attributes of an object key definition**

Attribute	Description
Column	Name of the column in full name notation.
IsReferencedColumn	Specifies whether the key column is required by other schema types for reference resolution The default value is <b>false</b> .
IsDNColumn	Specifies whether the value in this column is inserted as a component into the defined name of the object. The default value is <b>false</b> .
X500Abbreviation	Abbreviation that is added to the front of the value from this column when forming the defined name. Only required if IsDNColumn="true".

### Example

```
<Objectkey>
  <Key Column="APPLSYS.FND_APPLICATION.APPLICATION_ID" IsDNColumn="true"
    X500Abbreviation="AP" />
</Objectkey>
```

## Table definitions

The <Tables> tag can contain any number of table definitions in <Table> tags. This makes it possible to name all tables or view from which data for a single object of this schema type is required. The underlying required information for a table is defined in the attributes of the <Table> tag.

**Table 9: Attributes of a table definition**

Attribute	Description
Name	Name of the table (without schema name).
Schema	Name of the Oracle schema.

Attribute	Description
APK	Name of a column that can be an alternative primary key. This column is always loaded.
USN	Name of a column that stores information about the last object modifications. If the column <code>LAST_UPDATE_DATE</code> exists, this is used as change information by default and does not have to be specified explicitly.
WhereClause	WHERE clause for restricting the results set.
JoinParentTable	Name of a parent table when a join operation is carried out on a schema type higher up in the hierarchy.
JoinParentColumn	Comma-delimited list of columns in a parent table when a Join operation is carried out on a schema type higher up in the hierarchy (full notation).
JoinChildColumn	Comma-delimited list of columns in the currently defined table to be joined to the columns from <code>JoinParentColumn</code> in the Join operation (full notation). The sequence of columns in the list determines which columns are joined to each other.
View	Name of the view if there is a view for the table that filters the table contents based on the current database edition.  Example: Specify the <code>FND_RESPONSIBILITY_TL#</code> view for the <code>FND_RESPONSIBILITY_TL</code> table.

## Example

```
<Tables>
...
<Table Name="FND_RESPONSIBILITY_TL" View="FND_RESPONSIBILITY_TL#"
Schema="APPLSYS" APK="" USN="APPLSYS.FND_RESPONSIBILITY_TL.LAST_UPDATE_DATE"
WhereClause="APPLSYS.FND_RESPONSIBILITY_TL.LANGUAGE='$$SYSLANGU$'"
JoinParentColumn="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID,APPLSYS.FND_
RESPONSIBILITY.APPLICATION_ID" JoinParentTable="FND_RESPONSIBILITY"
JoinChildColumn="APPLSYS.FND_RESPONSIBILITY_TL.RESPONSIBILITY_ID,APPLSYS.FND_
RESPONSIBILITY_TL.APPLICATION_ID" />
...
</Tables>
```

## Primary key definition

The `<PK>` tags within the `<Table>` section name the primary key columns of a table. The name of the column is specified in the `Column` attribute. To define primary keys with multiple columns, enter each column in a separate tag. You can use any number of `<PK>` tags in a table definition.

**Table 10: Attribute of a primary key definition**

Attribute	Description
Column	Name of the primary key column (full notation).

### Example

```
<PK Column="APPLSYS.FND_RESPONSIBILITY_TL.RESPONSIBILITY_ID" />
```

## Column pairs in the hierarchy

The <ParentTableFK> tags within the <Table> section describe the column pairs that are to be equated with the table of the superordinate schema type in a Join operation.

**Table 11: Attributes of a column pair**

Attribute	Description
Column	Name of the column in the current defined table.
ParentColumn	Name of the column in the table of the superordinate schema type.

### Example

```
<ParentTableFK Column="APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID"  
ParentColumn="APPLSYS.FND_APPLICATION.APPLICATION_ID" />
```

## Example of a complete table definition

```
<Object SchemaName="ORA-Responsibility" ParentSchemaName="ORA-Application"  
DisplayPattern="%vrtDistinguishedName%" IsReadOnly="true" UseDistinct="false">  
  <ObjectKey>  
    <Key Column="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID"  
      IsDNColumn="true" IsReferencedColumn="true" X500Abbreviation="RE" />  
    <Key Column="APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID" />  
  </ObjectKey>  
  <Tables>  
    <Table Name="FND_RESPONSIBILITY" View="FND_RESPONSIBILITY#"  
      Schema="APPLSYS" APK="" USN="" WhereClause="" JoinParentTable=""  
      JoinParentColumn="" JoinChildColumn="" >  
      <PK Column="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID" />  
      <ParentTableFK Column="APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID"  
        ParentColumn="APPLSYS.FND_APPLICATION.APPLICATION_ID" />  
    </Table>  
  </Tables>  
</Object>
```

```

</Table>
<Table Name="FND_RESPONSIBILITY_TL" View="FND_RESPONSIBILITY_TL#"
Schema="APPLSYS" APK="" USN="APPLSYS.FND_RESPONSIBILITY_TL.LAST_UPDATE_
DATE" WhereClause="APPLSYS.FND_RESPONSIBILITY_TL.LANGUAGE=' $SYSLANGU$ '"
JoinParentColumn="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_
ID,APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID" JoinParentTable="FND_
RESPONSIBILITY" JoinChildColumn="APPLSYS.FND_APPLICATION.APPLICATION_
ID" >
    <PK Column="APPLSYS.FND_RESPONSIBILITY_TL.RESPONSIBILITY_ID" />
</Table>
<Table Name="FND_APPLICATION" View="FND_APPLICATION#" Schema="APPLSYS"
APK="" USN="" WhereClause="" JoinParentTable="FND_RESPONSIBILITY"
JoinParentColumn="APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID"
JoinChildColumn="APPLSYS.FND_APPLICATION.APPLICATION_ID" >
    <PK Column="APPLSYS.FND_APPLICATION.APPLICATION_ID" />
</Table>
</Tables>
</Object>

```

## Explanation

The definition above shows the declaration of the ORA-Responsibility schema type as it is used internally by the Oracle E-Business Suite connector.

The schema type is subordinate to the ORA-Application schema type in the hierarchy (ParentSchemaName). It has two object key columns (APPLSYS.FND\_RESPONSIBILITY.RESPONSIBILITY\_ID and APPLSYS.FND\_RESPONSIBILITY.APPLICATION\_ID), of which only one is included as a part of the distinguished name `IsDNCColumn="true"`. The column APPLSYS.FND\_RESPONSIBILITY.APPLICATION\_ID is a part of the DistinguishedName of the superordinate schema type, which is added automatically at the end.

For the selection of all properties, records from the tables FND\_RESPONSIBILITY, FND\_RESPONSIBILITY\_TL and FND\_APPLICATION are queried by a Join operation. The columns for the Join operation are specified in the relevant attributes JoinParentColumn and JoinChildColumn.

The description text is read from the table FND\_RESPONSIBILITY\_TL in the language specified by the database connection configuration. For this reason, the symbolic variable `$SYSLANGU$` is used in the Where clause. For more information, see [Symbolic variables in WHERE clauses](#) on page 49.

## Task definitions

The `<Functions>` tag enables you to define methods within the object definition that can be run for objects of the schema type. Each method runs any number of SQL functions.

The name of the XML tag for a method determines the method name. One or more functions are defined within the method section. These functions are run in a defined sequence when the corresponding method is called on an object of the schema type.

## Structure of the task definitions

```
<Functions>
  <Insert>
    <Function ... OrderNumber="1" >
      <Parameter ...>
    </Function>
    <Function ... OrderNumber="2" >
      <Parameter ...>
    </Function>
  </Insert>
  <Delete>
    <Function ...>
      <Parameter ...>
    </Function>
  </Delete>
</Functions>
```

In this example, the schema type has two methods, Insert and Delete. When Insert is called, two functions must be run that are placed in a fixed order based on their OrderNumber attribute. When the Delete method is called, only one defined function is run.

## Function definitions

The <Function> section defines the name, run sequence, and parameter settings of SQL function calls.

**Table 12: Attributes of a function definition**

Attribute	Description
Name	Name of the function. Full notation in the form <Schema name>.<Package name>.<Function name>.
OrderNumber	Numerical specification of the run sequence. The default value is <b>1</b> .

The function package that provides functions for the modification of user accounts (APPS.FND\_USER\_PKG) is a special case. Due to the permission restrictions when running the functions of this package, you may need to implement a wrapper package that changes the call context. The name of this wrapper package can be saved in the connection

configuration. It is replaced at runtime before running the function in the SQL block. The symbolic variable for the defined package name is `$ebsUserPackageName$`. For more information, see [Setting up an initial synchronization project](#) on page 23.

## Example

```
<Function Name="$ebsUserPackageName$.CreateUser" OrderNumber="1" >
```

## Parameter definitions

The `<Parameter>` tags define the parameters to be transferred to a function, together with their type and the source of the parameter value.

**Table 13: Attributes of a parameter definition**

Attribute	Description
Name	Name of the parameter in the function definition.
PropertyName	Name of the object property whose value is to be transferred (full notation). - OR - Fixed value, if PropertyType="FIX" is defined.
PropertyType	Data type Possible values: <ul style="list-style-type: none"> <li>• <b>CHAR</b>: Character string.</li> <li>• <b>DATE</b>: Date value. This value is converted as a valid date.</li> <li>• <b>FIX</b>: Fixed string value. The fixed value specified in the PropertyName attribute is always transferred.</li> <li>• <b>NUM</b>: Numerical value. The conversion does not permit any alpha-numeric characters.</li> </ul>
Mandatory	Specifies whether the parameter is mandatory. The default value is <b>false</b> .
NullValue	Value or character string to be transferred as the null value.  This input is required in order to fill parameters with values specifically defined in function packages or generally known in Oracle Database as a Null representation. This parameter is optional. By default, when a null value is detected in a mandatory parameter, the character string <b>null</b> is transferred. In this case, an optional parameter is not transferred to the function call.  In three cases, a null value definition makes sense: <ol style="list-style-type: none"> <li>a. Use of a constant defined in the function package, for example <code>\$ebsUserPackageName\$.null_number</code>. In this case, the name of the function package stored in the connection configuration is used</li> </ol>

Attribute	Description
	for user account modification, if the variable expression \$ebsUserPackageName\$ is detected.
	b. Use of a symbolic constant defined in the Oracle Database, for example <b>sysdate</b> .
	c. Use of a specific expression not equal to <b>null</b> , for example <b>to_date('-2', 'J')</b> .

### Example

```
<Parameter Name="start_date" PropertyName="APPS.FND_USER_RESP_GROUPS_DIRECT.START_DATE" PropertyType="DATE" Mandatory="TRUE" NullValue="sysdate" />
```

## Symbolic variables in WHERE clauses

The language version setting belongs to each configuration of a database connection for an Oracle E-Business Suite. Texts loaded from the database should be delivered in the set language version, if the texts are translated. This setting can be used in WHERE clauses with the symbolic variable \$SYSLANG\$. The variable is replaced by the actual set value before running the SQL statement.

### Example

```
<Table Name="FND_SECURITY_GROUPS_TL" Schema="APPLSYS" APK="" USN=""
WhereClause="APPLSYS.FND_SECURITY_GROUPS_TL.LANGUAGE='$SYSLANG$'"
JoinParentColumn="APPLSYS.FND_SECURITY_GROUPS.SECURITY_GROUP_ID"
JoinChildColumn="APPLSYS.FND_SECURITY_GROUPS_TL.SECURITY_GROUP_ID" >
```

## 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 **Oracle E-Business Suite > Basic configuration data > Target system types** category.
2. In the result list, select the **Oracle E-Business Suite** 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_EBSSystem).XObjectKey`
8. Save the changes.

#### **Related topics**

- [Synchronizing single objects](#) on page 54
- [Post-processing outstanding objects](#) on page 55

## **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 **Oracle E-Business Suite connector** server function to the Job server.

All Job servers must access the same E-Business Suite 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 E-Business Suite Job servers](#) on page 163

## **Running synchronization**

Synchronization is started using scheduled process plans. It is possible to start synchronization manually in the Synchronization Editor. You can simulate synchronization beforehand to estimate synchronization results and discover errors in the synchronization configuration. If synchronization stopped unexpectedly, you must reset the start information to be able to restart synchronization.

If you want to specify the order in which target systems are synchronized, use the start up sequence to run synchronization. In a start up sequence, you can combine start up configurations from different synchronization projects and specify the order in which they

are run. For more information about start up sequences, see the *One Identity Manager Target System Synchronization Reference Guide*.

## Detailed information about this topic

- [Starting synchronization](#) on page 52
- [Deactivating synchronization](#) on page 54
- [Displaying synchronization results](#) on page 53
- [Pausing handling of target system specific processes \(Offline mode\)](#) on page 59

# Starting synchronization

When you set up the initial synchronization project using the Launchpad, a default schedule for regular synchronization is created and assigned. Activate this schedule to synchronize on a regular basis.

### *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**.

You can also start synchronization manually if there is no active schedule.

### *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**.

**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.

## 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.

### **Related topics**

- [Configuring the synchronization log](#) on page 29
- [Troubleshooting](#) on page 57

# Deactivating 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 extent. 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**.

## **Related topics**

- [Pausing handling of target system specific processes \(Offline mode\)](#) on page 59

# 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 **E-Business Suite** 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.

## Detailed information about this topic

- [Configuring single object synchronization](#) on page 49

# Tasks following synchronization

After the synchronization of data from the target system into the One Identity Manager database, rework may be necessary. Check the following tasks:

- [Post-processing outstanding objects](#) on page 55

## 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 **Oracle E-Business Suite > Target system synchronization: Oracle E-Business Suite** category.

The navigation view lists all the synchronization tables assigned to the **Oracle E-Business Suite** 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 14: 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 <b>Outstanding</b> label is removed from the object.  This runs a target system specific process that triggers the provisioning process for the object.  Prerequisites: <ul style="list-style-type: none"> <li>• The table containing the object can be published.</li> <li>• The target system connector has write access to the target system.</li> </ul>
	Reset	The <b>Outstanding</b> 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.

**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.

## Adding custom tables to the target system synchronization

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

#### **To add tables to target system synchronization**

1. In the Manager, select the **Oracle E-Business Suite > Basic configuration data > Target system types** category.
2. In the result list, select the **Oracle E-Business Suite** 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.

#### **Related topics**

- [Post-processing outstanding objects](#) on page 55

## Troubleshooting

Synchronization Editor helps you to analyze and eliminate synchronization errors.

- **Simulating synchronization**  
The simulation allows you to estimate the result of synchronization. This means you can, for example, recognize potential errors in the synchronization configuration.
- **Analyzing synchronization**  
You can generate the synchronization analysis report for analyzing problems which occur during synchronization, for example, insufficient performance.
- **Logging messages**  
One Identity Manager offers different options for logging errors. These include the synchronization log, the log file for One Identity Manager Service, the logging of messages with NLOG, and similar.
- **Reset start information**  
If synchronization stopped unexpectedly, for example, because a server was not available, the start information must be reset manually. Only then can the synchronization be restarted.
- **Resetting revisions**  
It may also be necessary to process those objects during synchronization, whose change information has not been updated since the last synchronization. This might be required if changes to data were made without the change information for the object being updated, for example. This means, the change information for objects becomes older than that saved in the synchronization project. In such cases, the revision for a start up configuration can be reset.

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

## Related topics

- [Displaying synchronization results](#) on page 53

# 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**

- [Deactivating synchronization](#) on page 54

## Managing E-Business Suite user accounts and persons

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 an E-Business Suite system, 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. 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.

If you want to map identity data from the HR module of the Oracle E-Business Suite in One Identity Manager, the imported persons:

- Can be assigned to E-Business Suite user accounts as HR people.
- Can be linked to user accounts through automatic identity assignment, account definitions, or manually.

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

## Related topics

- [Setting up account definitions](#) on page 62
- [Assigning identities automatically to E-Business Suite user accounts](#) on page 80
- [Entering main data of E-Business Suite user accounts](#) on page 134
- [Linking E-Business Suite user accounts with imported identities](#) on page 86

# 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 E-Business Suite 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 account definitions](#) on page 63
- [Creating manage levels](#) on page 65
- [Creating mapping rules for IT operating data](#) on page 68
- [Entering IT operating data](#) on page 69
- [Assigning account definitions to identities](#) on page 71
- (Optional) [Assigning account definitions to target systems](#) on page 77

# Creating account definitions

## To create or edit an account definition

1. In the Manager, select the **Oracle E-Business Suite > 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.

## Main data for account definitions

Enter the following data for an account definition:

**Table 15: 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.
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.  Leave empty for E-Business Suite systems.
Description	Text field for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
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 <b>QER   CalculateRiskIndex</b> configuration parameter is set.  For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Service item	Service item through which you can request the account definition resource in the IT Shop. Assign an existing service

Property	Description
	item or add a new one.
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	<p>Specifies whether the account definition is automatically assigned to all internal identities. To automatically assign the account definition to all internal identity, use the <b>Enable automatic assignment to identities</b>. 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.</p> <p>To automatically remove the account definition assignment from all identities, use the <b>Disable automatic assignment to identities</b>. The account definition cannot be reassigned to identities from this point on. Existing account definition assignments remain intact.</p>
Retain account definition if permanently disabled	<p>Specifies the account definition assignment to permanently deactivated identities.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is disabled.</p>
Retain account definition if temporarily disabled	<p>Specifies the account definition assignment to temporarily deactivated identities.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is disabled.</p>
Retain account definition on deferred deletion	<p>Specifies the account definition assignment on deferred deletion of identities.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p>

Property	Description
	Option not set (default): The account definition assignment is not in effect. The associated user account is disabled.
Retain account definition on security risk	<p>Specifies the account definition assignment to identities posing a security risk.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated user account is disabled.</p>
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.
Entitlements can be inherited	<p>Specifies whether the user account can inherit E-Business Suite permissions through the identity. If this option is set, the user account inherits permissions through hierarchical roles or IT Shop requests.</p> <ol style="list-style-type: none"> <li>1. Example: An identity with an E-Business Suite user account is a member of a department. This department is assigned an E-Business Suite entitlement. If this option is set, the user account inherits this entitlement.</li> <li>2. Example: An identity with an E-Business Suite user account requests an E-Business Suite entitlement in the IT Shop. The request is approved and assigned. The user account only inherits this entitlement if this option is active.</li> </ol>

## 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 not 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 **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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.

## Main data for manage levels

Enter the following data for a manage level.

**Table 16: 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: <ul style="list-style-type: none"><li>• <b>Never</b>: Data is not updated. (Default)</li><li>• <b>Always</b>: Data is always updated.</li><li>• <b>Only initially</b>: Data is only determined at the start.</li></ul>
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 permanently disabled	Specifies whether user accounts of permanently deactivated 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.

Property	Description
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.

## Related topics

- [Invalid entitlement assignments](#) on page 127

# Creating mapping rules 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
- Identity
- Privileged user account.

### To create a mapping rule for IT operating data

1. In the Manager, select the **Oracle E-Business Suite > 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 | EBS | Accounts | MailTemplateDefaultValues** configuration parameter.

5. Save the changes.

## Entering 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

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.

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 **Oracle E-Business Suite > 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 disabled. User accounts marked as **Outstanding** will only be 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*.

## 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 **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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 in 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 **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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 account definitions](#) on page 63

## **Assigning account definitions to target systems**

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.

### ***To assign the account definition to a target system***

1. In the Manager, select the system in the **Oracle E-Business Suite > Systems** 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.

### **Detailed information about this topic**

- [Assigning identities automatically to E-Business Suite user accounts](#) on page 80

# Deleting account definitions

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 **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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 system in the **Oracle E-Business Suite > Systems** 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 **Oracle E-Business Suite > Basic configuration data > Account definitions > Account definitions** category.
  - b. Select an account definition in the result list.
  - c. Click  to delete an account definition.

## Assigning identities automatically to E-Business Suite user accounts

When you add a user account, an existing identity can automatically be assigned to it. 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 | EBS | PersonAutoFullsync** configuration parameter and select the required mode.
- If you want identities to be assigned outside synchronization, in the Designer, set the **TargetSystem | EBS | PersonAutoDefault** configuration parameter and select the required mode.




- In the **TargetSystem | EBS | PersonExcludeList** configuration parameter, define the user accounts for which no automatic assignment to identities shall take place.

Example:

ANONYMOUS|SYSADMIN|AUTOINSTALL|INITIAL SETUP|FEEDER SYSTEM|CONCURRENT

**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 E-Business Suite 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 | EBS | 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 E-Business Suite system. Ensure that the manage level to be used is entered as the default manage level.
  - Define the search criteria for identity assignment to this system.

#### **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.

## **Related topics**

- [Creating account definitions](#) on page 63
- [Assigning account definitions to target systems](#) on page 77
- [Changing the manage level in user accounts](#) on page 84
- [Editing search criteria for automatic identity assignment](#) on page 82

# 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 E-Business Suite system. 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 EBSSystem 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. In the Manager, select the **Oracle E-Business Suite > Systems** category.
2. Select the E-Business Suite system 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 17: Search criteria for user accounts**

Apply to	Identity column	User account column
E-Business Suite user accounts	E-Business Suite user account (CentralEBSAccount)	User name (UserName)
	Identity (Person)	HR person (UID_PersonEmployee)

5. Save the changes.

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

## Related topics

- [Assigning identities automatically to E-Business Suite user accounts](#) on page 80
- [Finding identities and directly assigning them to user accounts](#) on page 83

# Finding identities and directly assigning them to user accounts

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

- **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.

**NOTE:** To display disabled user accounts or deactivated identities in the view, enable the **Even locked accounts are mapped** option.

If you assign a deactivated identity to a user account, it might be locked or deleted depending on the configuration.

### *To apply search criteria to user accounts*

1. In the Manager, select the **Oracle E-Business Suite > Systems** category.
2. Select the E-Business Suite system in the result list.
3. Select the **Define search criteria for identity assignment** task.
4. At the bottom of the form, 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.

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

The assignment of identities to user accounts creates connected user accounts (**Linked** state). To create managed user accounts (**Linked configured** state), you can assign an account definition at the same time.

### ***To assign identities directly to user accounts***

- Click **Suggested assignments**.
  1. Click the **Selection** box of all user accounts to which you want to assign the suggested identities. Multi-select is possible.
  2. (Optional) Select an account definition in the **Assign this account definition** drop-down, and select a manage level in the **Assign this account manage level** drop-down.
  3. Click **Assign selected**.
  4. Confirm the security prompt with **Yes**.

The identities determined using the search criteria are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.
- OR -
- Click **No identity assignment**.
  1. Click **Select identity** for the user account to which you want to assign an identity. Select an identity from the drop-down.
  2. Click the **Selection** box of all user accounts to which you want to assign the selected identities. Multi-select is possible.
  3. (Optional) Select an account definition in the **Assign this account definition** drop-down, and select a manage level in the **Assign this account manage level** drop-down.
  4. Click **Assign selected**.
  5. Confirm the security prompt with **Yes**.

The identities displayed in the **Identity** column are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

### ***To remove assignments***

- Click **Assigned user accounts**.
  1. Click the **Selection** box of all the user accounts with the identity assignment you want to delete. Multi-select is possible.
  2. Click **Remove selected**.
  3. Confirm the security prompt with **Yes**.

The assigned identities are removed from the selected user accounts.

## **Changing the manage level in 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 **Oracle E-Business Suite > 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 **General** tab.
5. Save the changes.

### **Related topics**

- [General main data of E-Business Suite user accounts](#) on page 134

## **Assigning account definitions to linked user accounts**

An account definition can be subsequently assigned to user accounts with **Linked** status. This may be necessary, for example, if:

- Identities and user accounts were linked manually
- Automatic identity assignment is configured, but when a user account is inserted, no account definition is assigned in the E-Business Suite system.

### ***To select user accounts through account definitions***

1. Create an account definition.
2. Assign an account definition to the system.
3. Assign the account definition and manage level to user accounts in **linked** status.
  - a. In the Manager, select the **Oracle E-Business Suite > User accounts > Linked but not configured > <Host>** category.
  - b. Select the **Assign account definition to linked accounts** task.

### **Detailed information about this topic**

- [Assigning account definitions to target systems](#) on page 77

## **Manually linking identities to E-Business Suite user accounts**

An identity can be linked to multiple E-Business Suite user accounts, for example, so that you can assign an administrative user account in addition to the default user account. One

identity can also use default user accounts with different types.

### ***To manually assign user accounts to an identity***

1. In the Manager, select the **Identities > Identities** category.
2. Select the identity in the result list and run the **Assign E-Business Suite user accounts** task.
3. Assign the user accounts.
4. Save the changes.

### **Related topics**

- [Supported user account types](#) on page 88

## **Linking E-Business Suite user accounts with imported identities**

Identity data imported from Oracle E-Business Suite is mapped in the Person table in the One Identity Manager database. The data source of the import is specified for every imported identity (ImportSource column). The E-Business Suite user accounts have a variety of properties with which these identities can be assigned.

### ***To assign an imported identity to a user account***

1. In the Manager, select the **Oracle E-Business Suite > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Select the **General** tab.
5. Select the HR person from the **HR person** drop-down.
  - OR -
  - Select the customer from the **Customer** drop-down.
  - OR -
  - Select the supplier from the **Supplier** drop-down.
6. Save the changes.

If the imported identities are only connected to the user accounts through these columns, the user accounts are not managed by One Identity Manager. If an identity is deactivated or classified as a security risk, this change has no effect on the assigned user account. To utilize the possibilities available in One Identity Manager for the management of user accounts and identities for the imported identities, you can create connected user accounts. In these account, persons are connected to the user accounts by the `EBSUser.UID_Person` column.

HR people can also be connected to user accounts through automatic identity assignment. Standard search criteria are defined for this.

**Table 18: Identities assigned to user accounts**

Property	Description
Person (UID_Person)	<p>Identity that uses this user account.</p> <ul style="list-style-type: none"> <li>An identity is already entered if the user account was generated by an account definition.</li> <li>If you are using automatic identity assignment, an associated identity is found and added to the user account when you save the user account.</li> <li>If you create the user account manually, you can select an identity in the drop-down.</li> </ul> <p>The drop-down displays activated and deactivated identities by default. If you do not want to see any deactivated identities, set the <b>QER   Person   HideDeactivatedIdentities</b> configuration parameter.</p> <p><b>NOTE:</b> If you assign a deactivated identity to a user account, it might be locked or deleted depending on the configuration.</p> <p>Every identity can be assigned.</p>
Customer (UID_PersonCustomer)	<p>Reference to an identity that is listed as a customer.</p> <p>Only identities from the <b>E-Business Suite AR</b> data source can be assigned (Person.ImportSource='EBSOIM').</p>
HR person (UID_PersonEmployee)	<p>Reference to an identity in the Oracle E-Business Suite Human Resources module.</p> <p>Only identities from the <b>E-Business Suite HR</b> data source can be assigned (Person.ImportSource='EBSHR').</p>
Party (UID_PersonParty)	<p>Reference to an identity that is listed as a party.</p> <p>An identity with the <b>E-Business Suite AR</b> data source can be assigned (Person.ImportSource='EBSOIM'). The assignment cannot be edited in One Identity Manager.</p>
Supplier (UID_PersonSupplier)	<p>Reference to an identity that is listed as a supplier or a contact.</p> <p>Only identities from the <b>E-Business Suite AP</b> data source can be assigned (Person.ImportSource='EBSCRM').</p>

### Detailed information about this topic

- [Managing E-Business Suite user accounts and persons](#) on page 61
- [Editing search criteria for automatic identity assignment](#) on page 82

## Related topics

- [Setting up a synchronization project for identity data](#) on page 27
- [Setting up a synchronization project for organizational data](#) on page 28
- [HR people](#) on page 152
- [Parties](#) on page 154
- [Suppliers and contacts](#) on page 153

# Special features for the deletion of identities

If an identity is deleted in the One Identity Manager database who is connected to an E-Business Suite user account, the user account loses its reference to the identity after the deferred deletion has expired. If the user account is managed using an account definition, the behavior on deletion of the connected identity is defined in the account definition. User accounts cannot be deleted in One Identity Manager. The identity is physically deleted from the One Identity Manager database if all other prerequisites for deletion are in place. The user account is retained with the **INACTIVE** status.

For more information about deleting identities and user accounts, see the *One Identity Manager Target System Base Module Administration Guide*.

## Related topics

- [Deleting E-Business Suite user accounts](#) on page 142
- [Disabling E-Business Suite user accounts](#) on page 140

# 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 19: 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).

### Detailed information about this topic

- [Default user accounts](#) on page 89
- [Administrative user accounts](#) on page 90
- [Privileged user accounts](#) on page 93

## 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 settings are recommended for default user accounts:

- In the mapping rule for the `IsGroupAccount` column, use the default value **1** and enable 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.

## Related topics

- [Setting up account definitions](#) on page 62

# 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.

## Related topics

- [Providing an administrative user account for one identity](#) on page 91
- [Providing an administrative user account for multiple identities](#) on page 92

# Providing an administrative user account for one identity

Use this task to create an administrative user account that can be used by an identity.


## Prerequisites

- The user account must be labeled as a personalized administrator identity.
- The identity that will be using the user account must be marked as a personalized administrator identity.
- The identity that will be using the user account must be linked to a main identity.

### *To prepare an administrative user account for an identity*

1. Label the user account as a personalized administrator identity.
  - a. In the Manager, select the **Oracle E-Business Suite > User accounts** category.
  - b. Select the user account in the result list.
  - c. Select the **Change main data** task.
  - d. On the **General** tab, in the **Identity** selection list, select **Personalized administrator identity**.
2. Link the user account to the identity that will be using this administrative user account.

- a. In the Manager, select the **Oracle E-Business Suite > User accounts** category.
- b. Select the user account in the result list.
- c. Select the **Change main data** task.
- d. On the **General** tab, in the **Identity** selection list, select the identity that will be using this administrative user account.

**TIP:** If you are the target system manager, you can select  to create a new identity.

## Related topics

- [Providing an administrative user account for multiple identities](#) on page 92
- For more information about mapping identity, see the *One Identity Manager Identity Management Base Module Administration Guide*.

# Providing an administrative user account for multiple identities

Use this task to create an administrative user account that can be used by more than one identity.


## Prerequisites

- The user account must be labeled as a shared identity.
- There must be an identity with the type **Shared identity** available. The shared identity must have a manager.
- The identities who are permitted to use the user account must be labeled as a primary identity.

## To prepare an administrative user account for multiple identities

1. Label the user account as a shared identity.
  - a. In the Manager, select the **Oracle E-Business Suite > User accounts** category.
  - b. Select the user account in the result list.
  - c. Select the **Change main data** task.
  - d. On the **General** tab, in the **Identity** drop-down, select **Shared identity**.
2. Link the user account to an identity.
  - a. In the Manager, select the **Oracle E-Business Suite > User accounts** category.
  - b. Select the user account in the result list.

- c. Select the **Change main data** task.
- d. On the **General** tab, in the **Identity** drop-down, select an identity the type **Shared identity**.

**TIP:** If you are the target system manager, you can use the  button to create a new shared identity.

3. Assign the identities who will use this administrative user account to the user account.
  - a. In the Manager, select the **Oracle E-Business Suite > User accounts** category.
  - b. Select the user account in the result list.
  - c. Select the **Assign identities authorized to use** task.
  - d. 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 .

## Related topics

- [Providing an administrative user account for one identity](#) on page 91
- For more information about mapping identity, see the *One Identity Manager Identity Management Base Module Administration Guide*.

## 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` column 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.

- To use a prefix for the login name, in the Designer, set the **TargetSystem | EBS | Accounts | PrivilegedAccount | AccountName\_Prefix** configuration parameter.
- To use a postfix for the login name, in the Designer, set the **TargetSystem | EBS | Accounts | PrivilegedAccount | AccountName\_Postfix** configuration parameter.

These configuration parameters are evaluated in the default installation, if a user account is marked with the **Privileged user account** property (`IsPrivilegedAccount` column). The user account login names are renamed according to the formatting rules. This also occurs if the user accounts are labeled as privileged using the **Mark selected user accounts as privileged** schedule. If necessary, modify the schedule in the Designer.

## Related topics

- [Setting up account definitions](#) on page 62

## Login credentials

When new user accounts are created in One Identity Manager, the passwords needed to log in to the target system are created immediately also. Various options are available for assigning the initial password. Predefined password policies are applied to the passwords, and you can adjust these policies to suit your individual requirements if necessary. You can set up email notifications to distribute the login credentials generated to users.

### Detailed information about this topic

- [Password policies for E-Business Suite user accounts](#) on page 95
- [Initial password for new E-Business Suite user accounts](#) on page 106
- [Email notifications about login data](#) on page 107

## Password policies for E-Business Suite 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 policies 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 96
- [Using password policies](#) on page 97
- [Editing password policies](#) on page 98
- [Custom scripts for password requirements](#) on page 102
- [Editing the excluded list for passwords](#) on page 105

- [Checking passwords](#) on page 106
- [Testing the generation of passwords](#) on page 106

## 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 **E-Business Suite password policy** is predefined for Oracle E-Business Suite systems. You can apply this password policy to user accounts (`EBSUser.Password`) of an E-Business Suite system.

If the E-Business Suite systems' password requirements differ, you should set up your own password policies for each system.

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 **E-Business Suite password policy** is predefined for Oracle E-Business Suite systems. You can apply this password policy to user accounts (EBSUser.Password) of an E-Business Suite system.

If the E-Business Suite systems' password requirements differ, you should set up your own password policies for each system.

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 E-Business Suite system.
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 **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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 99
- [Policy settings](#) on page 99
- [Character classes for passwords](#) on page 101
- [Custom scripts for password requirements](#) on page 102

# General main data of password policies

Enter the following main data of a password policy.

**Table 20: 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.  <b>NOTE:</b> The <b>One Identity Manager password policy</b> 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.

## Policy settings

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

**Table 21: 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

Property	Meaning
	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 <b>0</b> , 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 <b>256</b> .
Max. errors	<p>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 <b>0</b>, the number of failed logins is not taken into account.</p> <p>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.</p> <p>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 <i>One Identity Manager Web Portal User Guide</i>.</p>
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires. If the value is <b>0</b> , then the password does not expire.
Password history	Enter the number of passwords to be saved. If, for example, a value of <b>5</b> is entered, the user's last five passwords are stored. If the value is <b>0</b> , 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 <b>0</b> means that the password strength is not tested. The values <b>1</b> , <b>2</b> , <b>3</b> and <b>4</b> specify the required complexity of the password. The value <b>1</b> represents the lowest requirements in terms of password strength. The value <b>4</b> 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 <b>Contains name properties for</b>

Property	Meaning
	<b>password check</b> option is set. In the Designer, adjust this option in the column definition. For more information, see the <i>One Identity Manager Configuration Guide</i> .

## Character classes for passwords

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

**Table 22: Character classes for passwords**

Property	Meaning
Required number of character classes	<p>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 <b>Min. number letters</b>, <b>Min. number lowercase</b>, <b>Min. number uppercase</b>, <b>Min. number digits</b>, and <b>Min. number special characters</b>.</p> <p>That means:</p> <ul style="list-style-type: none"> <li>• Value <b>0</b>: All character class rules must be fulfilled.</li> <li>• Value <b>&gt;0</b>: Minimum number of character class rules that must be fulfilled. At most, the value can be the number of rules with a value <b>&gt;0</b>.</li> </ul> <p>  <b>NOTE:</b> Generated passwords are not tested for this.</p>
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.
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	Specifies the maximum number of identical characters that can be present in the password in total.

Property	Meaning
characters 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 103
- [Generating passwords with a script](#) on page 104

## 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 **Oracle E-Business Suite > 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 104

# 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 **Oracle E-Business Suite > 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 103

## **Editing the excluded list for passwords**

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

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

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

1. 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 passwords

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 **Oracle E-Business Suite > 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 the generation of passwords

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 **Oracle E-Business Suite > 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 E-Business Suite user accounts

You can issue an initial password for a new E-Business Suite 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 | EBS | 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 E-Business Suite user accounts](#) on page 95
- [Email notifications about login data](#) on page 107

# Email notifications about login data

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.

The following prerequisites must be fulfilled in order to use notifications:

- Ensure that the email notification system is configured in One Identity Manager. For more information, see the *One Identity Manager Installation Guide*.
- In the Designer, set the **Common | MailNotification | DefaultSender** configuration parameter and enter the sender address for sending the email notifications.
- 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*.
- 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 data by email**

1. In the Designer, set the **TargetSystem | EBS | Accounts | InitialRandomPassword** configuration parameter.

2. In the Designer, set the **TargetSystem | EBS | Accounts | InitialRandomPassword | SendTo** configuration parameter and enter the message recipient as a value.

If no recipient can be found, the email is sent to the address stored in the **TargetSystem | EBS | DefaultAddress** configuration parameter.

3. In the Designer, set the **TargetSystem | EBS | 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 | EBS | 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.

## Managing entitlement assignments

E-Business Suite User accounts are assigned permissions for objects Oracle E-Business Suite by means of responsibilities. Responsibilities cannot be assigned to user accounts directly. Instead, they are inherited by means of security groups. Permissions in Oracle E-Business Suite are characterized by the combination of responsibilities and security groups. These combinations are mapped in the One Identity Manager database as E-Business Suite permissions.

In Oracle E-Business Suite, entitlements can be assigned to user accounts directly and indirectly. Multiple indirect assignments with different validity periods can exist. Indirect assignments are imported into One Identity Manager and can be used for evaluations and reports. Direct assignments are also imported. For each user account there can be only one direct assignment.

In One Identity Manager, E-Business Suite entitlements can also be assigned directly or indirectly. Entitlement assignments made in One Identity Manager are transferred to Oracle E-Business Suite as direct assignments. The system then determines the assignment with the effective validity period out of all the entitlement assignments for a user account.

In the One Identity Manager database, direct, and indirect entitlement assignments are identified as follows.

**Table 23: Identification of direct and indirect entitlement assignments in EBSUserInResp table**

Assignment origin	Type of assignment	Indirect (Column OriginIndirect)	Origin (Column XOrigin)
Oracle E-Business Suite	Indirect	1 (yes)	1
	Direct	0 (no)	1
One Identity Manager	Direct	0 (no)	1
	Indirect	0 (no)	2
	Ineffective	0 (no)	16

For more information about calculating assignments in One Identity Manager, see the *One Identity Manager Identity Management Base Module Administration Guide*.

### Detailed information about this topic

- [Assigning E-Business Suite entitlements to user accounts in One Identity Manager](#) on page 110
- [Validity period of permission assignments](#) on page 120

## Assigning E-Business Suite entitlements to user accounts in One Identity Manager

In One Identity Manager, E-Business Suite entitlements can be assigned directly or indirectly to identities. In the case of indirect assignment, identities and entitlements are organized in hierarchical roles. The number of entitlements assigned to an identity is calculated from the position in the hierarchy and the direction of inheritance. If the identity has an E-Business Suite user account, the entitlements are assigned to this user account.

Entitlements can also be assigned to identities through IT Shop requests. To enable the assignment of entitlements using IT Shop requests, identities are added as customers in a shop. All entitlements assigned to this shop as products can be requested by the customers. After approval is granted, requested entitlements are assigned to the identities.

You can use system roles to group entitlements together and assign them to identities as a package. You can create system roles that contain only E-Business Suite entitlements. You can also group any number of company resources into a system role.

To react quickly to special requests, you can also assign the E-Business Suite entitlements directly to user accounts.

For more information see the following guides:

Topic	Guide
Basic principles for assigning and inheriting company resources	<i>One Identity Manager Identity Management Base Module Administration Guide</i> <i>One Identity Manager Business Roles Administration Guide</i>
Assigning company resources through IT Shop requests	<i>One Identity Manager IT Shop Administration Guide</i>
System roles	<i>One Identity Manager System Roles Administration Guide</i>

## Detailed information about this topic

- [Validity period of permission assignments](#) on page 120
- [Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts](#) on page 111
- [Assigning E-Business Suite entitlements to departments, cost centers, and locations](#) on page 112
- [Assigning E-Business Suite entitlements to business roles](#) on page 113
- [Assigning E-Business Suite user accounts directly to an entitlement](#) on page 117
- [Adding E-Business Suite entitlements to system roles](#) on page 114
- [Adding E-Business Suite entitlements to the IT Shop](#) on page 115
- [Assigning E-Business Suite entitlements directly to a user account](#) on page 118

# Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts

In the case of indirect assignment, identities and E-Business Suite entitlements are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. When assigning E-Business Suite entitlements indirectly, check the following settings and modify them if necessary.

1. Assignment of identities and E-Business Suite entitlements is permitted for role classes (departments, cost centers, locations, or business roles).

For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

### ***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.
  2. Settings for assigning E-Business Suite entitlements to E-Business Suite user accounts.
    - E-Business Suite user accounts are labeled with the **Groups can be inherited** option.
    - E-Business Suite user accounts are linked with an identity through the UID\_Person (**Person**) column.
    - E-Business Suite user accounts and E-Business Suite entitlements belong to the same E-Business Suitesystem.

**NOTE:** There are other configuration settings that play a role when company resources are inherited through departments, cost centers, locations, and business roles. For example, role inheritance might be blocked or inheritance of identities not allowed. For more information about the basic principles for assigning company resources, see the *One Identity Manager Identity Management Base Module Administration Guide*.

## Related topics

- [Entering main data of E-Business Suite user accounts](#) on page 134
- [General main data of E-Business Suite user accounts](#) on page 134
- [Entering main data of E-Business Suite entitlements](#) on page 143
- [General main data of an E-Business Suite entitlement](#) on page 143

# Assigning E-Business Suite entitlements to departments, cost centers, and locations


Assign the entitlement to departments, cost centers, and locations in order to assign entitlements to user accounts through these organizational entities.

***To assign a permission to a department, cost center or location (non role-based login):***

1. In the Manager, select the **Oracle E-Business Suite > entitlements** category.
2. Select the entitlements 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 permissions 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 E-Business Suite entitlements** task.

4. In the **Add assignments** pane, assign the entitlements.

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

**To remove an assignment**

- Select the entitlement and double-click .

5. Save the changes.

**Related topics**

- [Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts](#) on page 111
- [One Identity Manager users for managing Oracle E-Business Suite](#) on page 10

## Assigning E-Business Suite entitlements to business roles

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

You assign entitlements to business roles so that these entitlements are assigned to user accounts through these business roles.

**To assign an entitlement to business roles (non role-based login):**


1. In the Manager, select the **Oracle E-Business Suite > entitlements** category.

2. Select the entitlements 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 entitlements to a business role (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 E-Business Suite entitlements** task.
4. In the **Add assignments** pane, assign the entitlements.

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

**To remove an assignment**

- Select the entitlement and double-click .

5. Save the changes.

## Related topics

- [Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts](#) on page 111
- [One Identity Manager users for managing Oracle E-Business Suite](#) on page 10

# Adding E-Business Suite entitlements to system roles

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

Use this task to add an entitlement to system roles. If you assign a system role to identities, all user accounts owned by these identities inherit the entitlement.

**NOTE:** Groups with the **Only use in IT Shop** option can only be assigned to system roles that also have this option set. For more information, see the *One Identity Manager System Roles Administration Guide*.

**To assign a group to system roles:**

1. In the Manager, select the **Oracle E-Business Suite > entitlements** category.
2. Select the entitlements 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.

## Related topics

- [Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts](#) on page 111

# Adding E-Business Suite entitlements to the IT Shop

When you assign a permission 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 permissions must be labeled with the **IT Shop** option.
- The permission 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 permission easier to find in the Web Portal, assign a service category to the service item.

- If you only want the permission to be assigned to identities through IT Shop requests, the permissions 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 permissions to IT Shop shelves. Target system administrators are not authorized to add permissions to IT Shop.

### **To add a permission to the IT Shop.**

1. In the Manager, select the **Oracle E-Business Suite > Entitlements** (non role-based login) category.  
- OR -  
In the Manager, select the **Entitlements > E-Business Suite entitlements** (role-based login) category.
2. In the result list, select the permission.
3. Select the **Add to IT Shop** task.

4. To assign the entitlement to shelves, select the **IT Shop shelves** tab and, in the **Add assignments** section, double-click on the shelves.
5. To assign the entitlement to IT Shop templates, select the **IT Shop templates** tab and, in the **Add assignments** section, double-click on the templates.
6. Save the changes.

#### ***To remove, an entitlement from individual shelves of the IT Shop***

1. In the Manager, select the **Oracle E-Business Suite > Entitlements** (non role-based login) category.  
- OR -  
In the Manager, select the **Entitlements > E-Business Suite entitlements** (role-based login) category.
2. In the result list, select the permission.
3. Select the **Add to IT Shop** task.
4. To remove the entitlement from the shelves, select the **IT Shop shelves** tab and, in the **Remove assignments** section, double-click the shelves.
5. To remove the entitlement 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 entitlement from all shelves of the IT Shop***

1. In the Manager, select the **Oracle E-Business Suite > Entitlements** (non role-based login) category.  
- OR -  
In the Manager, select the **Entitlements > E-Business Suite entitlements** (role-based login) category.
2. In the result list, select the permission.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

The entitlement is removed from all shelves by the One Identity Manager Service. All requests and assignment requests with this entitlement 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 an E-Business Suite entitlement](#) on page 143
- [Prerequisites for indirect assignment of E-Business Suite entitlements to E-](#)

[Business Suite user accounts](#) on page 111

- [One Identity Manager users for managing Oracle E-Business Suite](#) on page 10

## Assigning E-Business Suite user accounts directly to an entitlement

To react quickly to special requests, you can assign the entitlements directly to user accounts.

### *To assign an entitlement directly to user accounts*

1. In the Manager, select the **Oracle E-Business Suite > entitlements** category.
2. Select the entitlements in the result list.
3. Select the **Assign user accounts** task.

The top area of the form displays all user accounts that have already been assigned, together with their validity periods. The overview shows the user accounts that have been assigned both directly and indirectly. For direct assignments, an **Active from (direct)** date is set; indirect assignments do not have a direct validity date.

### *To assign the entitlement to a user account:*

1. Click **Add**.
2. Select the user account from the **User account** drop-down.
3. In the **Active from (direct)** input field, enter the first date from on the direct entitlement assignment is valid.
4. (Optional) In the **Active to (direct)** input field, enter the last date on which the direct entitlement assignment is valid.
5. (Optional) Add further user accounts.
6. Save the changes.

### *To edit a direct entitlement assignment*

1. In the overview, select the direct entitlement assignment that you want to edit.
2. Change the values in the input fields **Active from (direct)**, **Active to (direct)**, or **Description**.
3. Save the changes.

Only direct assignments can be edited. If you select and edit an indirect assignment in the overview, this creates an additional direct assignment.

Entitlement assignments cannot be deleted. Instead, there are two options for indicating that a direct assignment is no longer valid.

- Enter the current date as the expiration date of the entitlement.  
Select this option, for example, if an entitlement assignment will become invalid on a defined date in the future.  
- OR -
- Delete the entitlement assignment.  
Select this option, for example, if an inherited entitlement assignment also exists alongside the direct assignment, and you want the inherited entitlement assigned to replace the direct assignment.

### **To set the expiration date for a direct entitlement assignment**

1. In the overview, select the direct entitlement assignment that you no longer want to be effective.
2. Next to the input field **Active to (direct)**, click ....
3. Click **Today** or define a different expiration date.
4. Save the changes.

### **To remove a direct entitlement assignment**

1. In the overview, select the direct entitlement assignment that you no longer want to be effective.
2. Click **Delete**.
3. Save the changes.

The first and last validity date of the direct assignment (**Active from (direct)** and **Active to (direct)**) are deleted. The final validity date (**Active to (effective)**) is recalculated. If no further valid assignments exist, the final validity date is set to a date in the past and X0rigin is assigned the value 16.

### **Detailed information about this topic**

- [Validity period of permission assignments](#) on page 120

### **Related topics**

- [Invalid entitlement assignments](#) on page 127

## **Assigning E-Business Suite entitlements directly to a user account**

To react quickly to special requests, you can assign entitlements directly to a user account. You cannot directly assign permissions that have the **Only use in IT Shop** option set.

### ***To assign entitlements directly to a user account***

1. In the Manager, select the **Oracle E-Business Suite > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign permission** task.

The top area of the form displays all entitlements that have already been assigned, together with their validity periods. The overview shows the entitlements that have been assigned both directly and indirectly. For direct assignments, an **Active from (direct)** date is set; indirect assignments do not have a direct validity date.

### ***To assign an entitlement to the user account***

1. Click **Add**.
2. Select the entitlement you want to assign from the **E-Business Suite Entitlement** drop-down.
3. In the **Active from (direct)** input field, enter the first date from on the direct entitlement assignment is valid.
4. (Optional) In the **Active to (direct)** input field, enter the last date on which the direct entitlement assignment is valid.
5. (Optional) Add further entitlements.
6. Save the changes.

### ***To edit a direct entitlement assignment***

1. In the overview, select the direct entitlement assignment that you want to edit.
2. Change the values in the input fields **Active from (direct)**, **Active to (direct)**, or **Description**.
3. Save the changes.

Only direct assignments can be edited. If you select and edit an indirect assignment in the overview, this creates an additional direct assignment.

Entitlement assignments cannot be deleted. Instead, there are two options for indicating that a direct assignment is no longer valid.

- Enter the current date as the expiration date of the entitlement.  
Select this option, for example, if an entitlement assignment will become invalid on a defined date in the future.  
- OR -
- Delete the entitlement assignment.  
Select this option, for example, if an inherited entitlement assignment also exists alongside the direct assignment, and you want the inherited entitlement assigned to replace the direct assignment.

### **To set the expiration date for a direct entitlement assignment**

1. In the overview, select the direct entitlement assignment that you no longer want to be effective.
2. Next to the input field **Active to (direct)**, click ...
3. Click **Today** or define a different expiration date.
4. Save the changes.

### **To remove a direct entitlement assignment**

1. In the overview, select the direct entitlement assignment that you no longer want to be effective.
2. Click **Delete**.
3. Save the changes.

The first and last validity date of the direct assignment (**Active from (direct)** and **Active to (direct)**) are deleted. The final validity date (**Active to (effective)**) is recalculated. If no further valid assignments exist, the final validity date is set to a date in the past and XOrigin is assigned the value 16.

### **Detailed information about this topic**

- [Validity period of permission assignments](#) on page 120

### **Related topics**

- [Invalid entitlement assignments](#) on page 127
- [Adding E-Business Suite entitlements to the IT Shop](#) on page 115

## **Validity period of permission assignments**

You can limit the time for which permission assignments are valid. A user account can receive permissions by direct assignment as well as through a variety of different inheritance paths. Each of these assignments can have a different validity period. One Identity Manager uses all validity periods to determine the actual validity period effective at the current time. This calculation considers all assignments with `OriginIndirect = 0`.

**Table 24: Properties of a permission assignment**

<b>Property</b>	<b>Description</b>
Active from	First date from which the assignment is valid. This date is calculated from

Property	Description
(effective)	all assignments (direct and indirect).
Active to (effective)	Last date on which the assignment is valid This date is calculated from all assignments (direct and indirect). If no date is specified, the assignment is unlimited.
Active from (direct)	First date from which the direct assignment is valid
Active to (direct)	Last date on which the direct assignment is valid If no date is specified, the assignment is unlimited.
Indirect	Specifies whether this assignment maps an indirect permission from the target system. You cannot edit indirect assignments in One Identity Manager.
Description	Text field for additional explanation.

## Calculation of the effective validity period

In One Identity Manager, one user account-permission combination can have multiple assignments with different validity periods. However, only the effective assignment is transferred to Oracle E-Business Suite. One Identity Manager calculates the effective validity period from all the assignments. The different assignment types are incorporated into the calculation as follows:

**Table 25: Determine validity period**

Type of assignment	Validity period
Direct assignment	<b>Active from (direct)</b> and <b>Active to (direct)</b>
Request	Validity period of the request when the <b>Valid from</b> date of the request has been reached or exceeded.  For unlimited requests, 01.01.1900 is entered at the first validity date.
assignment request	Validity period of the request when the <b>Valid from</b> date of the request has been reached or exceeded.  For unlimited requests, 01.01.1900 is entered at the first validity date.
Inheritance by department, location, cost center, or business role (not an assignment request)	Unlimited only  The date of the assignment is set as the first date of the validity.
Inheritance through dynamic role	Unlimited only

Type of assignment	Validity period
	The date of the assignment is set as the first date of the validity.
Inheritance by system role	Unlimited only The date of the assignment is set as the first date of the validity.

The effective assignment is controlled by a schedule.

- **Active from (effective)**: earliest initial validity date of all the assignments
- **Active to (effective)**: latest last validity date of all limited assignments  
If the assignment is unlimited, **Active to (effective)** is empty.

### Detailed information about this topic

- [Assigning E-Business Suite entitlements to user accounts in One Identity Manager](#) on page 110

### Related topics

- [Invalid entitlement assignments](#) on page 127

## Effectiveness of entitlement assignments

When E-Business Suite entitlements are assigned to user accounts an identity may obtain two or more groups that are not permitted in this combination. To prevent this, you can declare mutually exclusive entitlements. To do this, you specify which of the two entitlements should become active on user accounts if both are assigned.

It is possible to assign an excluded entitlements directly, indirectly, or by IT Shop request at any time. One Identity Manager determines whether the assignment is effective.

#### NOTE:

- You cannot define a pair of mutually exclusive entitlements. This means that the definition "Entitlement A excludes entitlement B" AND "Entitlement B excludes entitlement A" is not permitted.
- Each entitlement to be excluded from another entitlement must be declared separately. Exclusion definitions cannot be inherited.

The effectiveness of the assignments is stored in the EBSUserInResp table using the ValidTo and XOrigin columns, and in the BaseTreeHasEBSResp table, using the XIsInEffect column.

## Example of the effectiveness of entitlements

- The entitlements A, B, and C are defined in an E-Business Suite system.
- Entitlement A is assigned through the "Marketing" department, entitlement B through the "Finance" department, and entitlement C through the "Control group" business role.

Jo User1 has a user account in this system. 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 entitlements A, B, and C.

You must use appropriate measures to ensure that an identity cannot obtain entitlements A and B at the same time. This means that entitlements A and B are mutually exclusive. A user with entitlement C also cannot be assigned entitlement B. Entitlements B and C are therefore mutually exclusive.

**Table 26: Definition of excluded entitlements (EBSRespExclusion table)**

Effective entitlement	Excluded entitlement
Entitlement A	
Entitlement B	Entitlement A
Entitlement C	Entitlement B

**Table 27: Effective assignments**

Identity	Member in role	Effective entitlement
Pat Identity1	Marketing	Entitlement A
Jan User3	Marketing, finance	Entitlement B
Jo User1	Marketing, finance, control group	Entitlement C
Chris User2	Marketing, control group	Entitlement A Entitlement C

Only the entitlement C assignment is in effect for Jo User1 and is published in the target system. If Jo User1 leaves the "control group" business role at a later date, entitlement B also takes effect.

Entitlements A and C are in effect for Chris User2 because no exclusions are defined between these two entitlements. If this should not be allowed, define a further exclusion for entitlement C.

**Table 28: Excluded entitlements and effective assignments**

Identity	Member in role	Assigned entitlement	Excluded entitlement	Effective entitlement
Chris User2	Marketing	Entitlement A		Entitlement C
	Control group	Entitlement C	Entitlement B Entitlement A	

## Prerequisites

- The **QER | Structures | Inherit | 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 entitlements belong to the same E-Business Suite system.

## To exclude entitlements

1. In the Manager, select the **Oracle E-Business Suite > entitlements** category.
2. Select an entitlement in the result list.
3. Select the **Exclude E-Business Suite entitlements** task.
4. In the **Add assignments** pane, assign entitlements that are mutually exclusive to the entitlement.

- OR -

In the **Remove assignments** pane, remove the entitlements that are no longer mutually exclusive.

5. Save the changes.

## Related topics

- [Invalid entitlement assignments](#) on page 127

# Inheritance of E-Business Suite entitlements based on categories

In One Identity Manager, user accounts can selectively inherit entitlements. To do this, entitlements, 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. In the other tables, enter your categories for the permissions. Each table contains the category positions **position 1** to **position 63**.

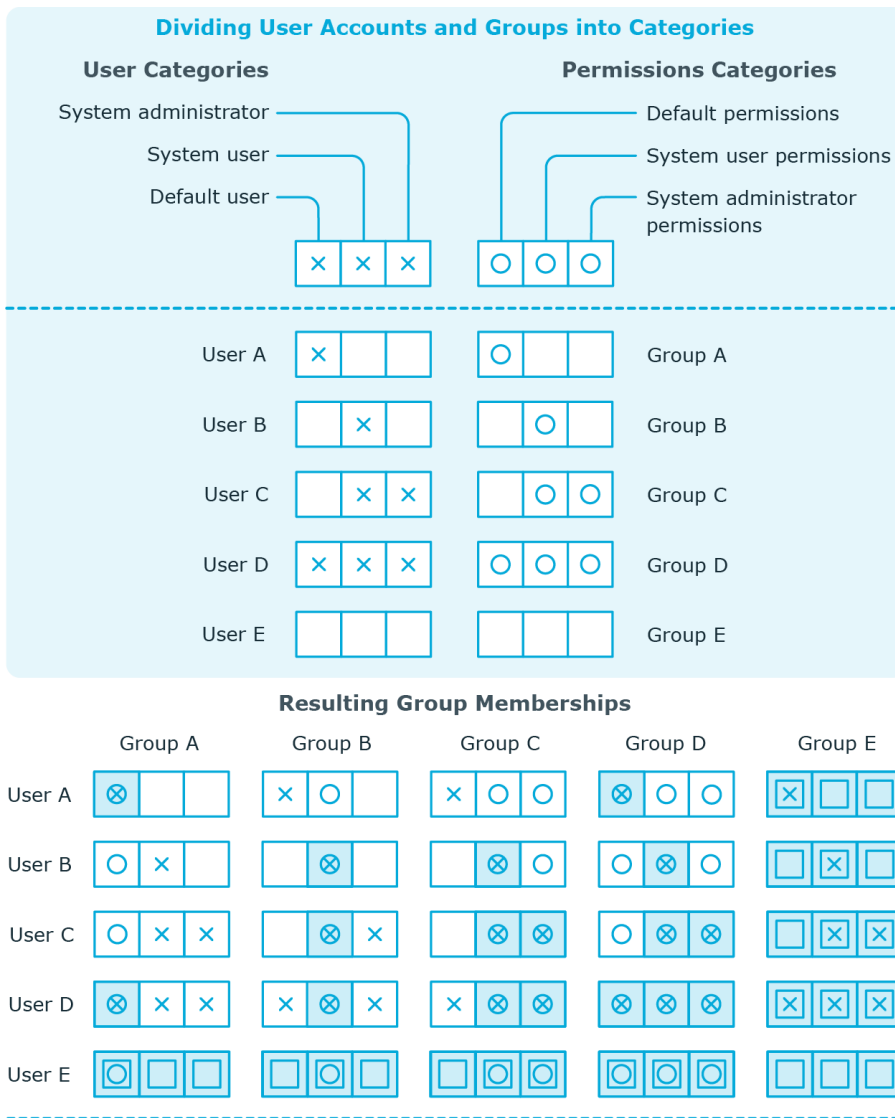
Every user account can be assigned to one or more categories. Each entitlement can also be assigned to one or more categories. If at least one of the category items between the user account and the assigned entitlement is the same, the entitlement is inherited by the user account. If the entitlement or the user account is not classified in a category, the entitlement is also inherited by the user account.

**NOTE:** Inheritance through categories is only taken into account when entitlements are assigned indirectly through hierarchical roles. Categories are not taken into account when entitlements are directly assigned to user accounts.

**Table 29: Category examples**

<b>Category position</b>	<b>Categories for user accounts</b>	<b>Categories for permissions</b>
1	Default user	Default entitlements
2	System users	System user entitlements
3	System administrator	System administrator entitlements

**Figure 2: Example of inheriting through categories.**



**Key:**

<p> Inherits due to matching categories</p> <p> Inherits because user account is not categorized</p>	<p> Inherits because user account and group are not categorized</p> <p> Inherits because group is not categorized</p>
--	---

**To use inheritance through categories**

1. Define the categories in the E-Business Suite system.
2. Assign categories to user accounts through their main data.
3. Assign categories to entitlements through their main data.

## Related topics

- [Defining categories for the inheritance of E-Business Suite entitlements](#) on page 132
- [General main data of E-Business Suite user accounts](#) on page 134
- [General main data of an E-Business Suite entitlement](#) on page 143

# Invalid entitlement assignments

Entitlement assignments cannot be deleted. Different inheritance processes in One Identity Manager can cause an entitlement assignment to become invalid. The following processes may be responsible for this:

- Cancellation of a requested entitlement assignment or reaching the expiration date of an assignment
- Removal of a direct entitlement assignment in One Identity Manager
- Deletion of the assignment of an entitlement to hierarchical or dynamic roles or system roles
- Deletion of the user account's membership in hierarchical or dynamic roles
- Deletion of the assignment of a user account to system roles
- Exclusion of entitlements
- Changes to the category to which a user account or an entitlement is classified
- Disabling/deletion/security risk to identities and handling of user accounts through an account definition

For user accounts with the **Full managed** manage level, the account definition defines how entitlement assignments are handled if the identity is classified as a security risk, or the identity is disabled or marked for deletion. If you do not want to retain the entitlement assignments, they are marked as invalid.

- Disabling user accounts

If the user account is managed by an account definition, the account definition defines how entitlement assignments are handled. If you do not want to retain the entitlement assignments, they are marked as invalid.

For invalid entitlement assignments, the validity period is in the past. If the assignments are inherited or requested, or if an entitlement assignment is deleted in the Manager, XOrigin is assigned a value of **16**.

If the cause of a entitlement assignment becoming invalid is resolved, the final validity date and XOrigin are reset to their original values.

## Related topics

- [Effectiveness of entitlement assignments](#) on page 122
- [Main data for manage levels](#) on page 67

- [Main data for account definitions](#) on page 63
- [Assigning E-Business Suite entitlements to departments, cost centers, and locations](#) on page 112
- [Assigning E-Business Suite entitlements to business roles](#) on page 113
- [Adding E-Business Suite entitlements to system roles](#) on page 114
- [Inheritance of E-Business Suite entitlements based on categories](#) on page 125


## 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 3: Toolbar of the Overview of all assignments report.**



**Table 30: 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.

## Mapping E-Business Suite objects in One Identity Manager

You use One Identity Manager to manage all objects of the Oracle E-Business Suite, that are required for the optimization of access control in the target system. These objects are imported into the One Identity Manager database during synchronization. You cannot display or edit their properties in the Manager.

### E-Business Suite systems

An E-Business Suite system represent the target system of the synchronization of an Oracle E-Business Suite in One Identity Manager. E-Business Suite systems used to configure provisioning processes, for automatic assignment of identities to user accounts, and to pass down permissions to user accounts within an Oracle E-Business Suite.

**NOTE:** The Synchronization Editor sets up the E-Business Suite systems in the One Identity Manager database.


#### **To set up a system:**

1. In the Manager, select the **Oracle E-Business Suite > Systems** category.
2. Select the system in the result list.
3. Select the **Change main data** task.
4. Edit the main data of the system.
5. Save the changes.

### General main data of E-Business Suite systems

On the **General** tab, you enter the following main data:

**Table 31: General main data of E-Business Suite systems**

Property	Description
Display name	Name of the system to be displayed on the user interface
Account definition (initial)	<p>Initial account definition for creating user accounts. This account definition is used if automatic assignment of identities to user accounts is used for this system and if user accounts are to be created that are already managed (<b>Linked configured</b>). The account definition's default manage level is applied.</p> <p>User accounts are only linked to the identity (<b>Linked</b>) if no account definition is given. This is the case on initial synchronization, for example.</p>
Target system managers	<p>Application role, in which target system managers are specified for the system. Target system managers only edit the objects from systems to which they are assigned. A different target system manager can be assigned to each system.</p> <p>Select the One Identity Manager application role whose members are responsible for administration of this system. Use the  button to add a new application role.</p>
Synchronized by	<p>Type of synchronization through which data is synchronized between the system and One Identity Manager. You can no longer change the synchronization type once objects for this system are present in One Identity Manager.</p> <p>When you create system using the Synchronization Editor, <b>One Identity Manager</b> is used.</p>

**Table 32: Permitted values**

Value	Synchronization by	Provisioned by
One Identity Manager	Oracle E-Business Suite connector	Oracle E-Business Suite connector
No synchronization	none	none

**NOTE:** If you select **No synchronization**, you can define custom processes to exchange data between One Identity Manager and the target system.

Distinguished name	Unique name for the system in X509 syntax.
--------------------	--

**Related topics**


- [Assigning account definitions to target systems](#) on page 77
- [Setting up account definitions](#) on page 62

- [Assigning identities automatically to E-Business Suite user accounts](#) on page 80
- [Target system managers](#) on page 168

## Defining categories for the inheritance of E-Business Suite entitlements

In One Identity Manager, user accounts can selectively inherit entitlements. To do this, entitlements, 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. In the other tables, enter your categories for the permissions. Each table contains the category positions **position 1** to **position 63**.

### *To define a category*

1. In the Manager, select the system in the **Oracle E-Business Suite > Systems** 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 entitlements in the login language that you use.
7. Save the changes.

### Detailed information about this topic

- [Inheritance of E-Business Suite entitlements based on categories](#) on page 125

## Editing the synchronization project for an E-Business Suite system

Synchronization projects in which a system 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. In the Manager, select the **Oracle E-Business Suite > Systems** category.
2. Select the system in the result list.
3. Select the **Change main data** task.
4. Select the **Edit synchronization project** task.

### **Related topics**

- [Customizing the synchronization configuration](#) on page 30

## **E-Business Suite user accounts**

You use One Identity Manager to manage Oracle E-Business Suite user accounts. A user can log on to the E-Business Suite using their Oracle E-Business Suite user account. The user retains all permissions and security groups assigned to the user account. In addition, user accounts can also be linked to identities that are managed in the Oracle E-Business Suite. Identity data from the Oracle E-Business Suite can be synchronized with the One Identity Manager database and linked to the 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 E-Business Suite user account and obtain their IT operating data through assignment to a primary department, a primary location, or a primary cost center.

### **Related topics**

- [Managing E-Business Suite user accounts and persons](#) on page 61
- [Setting up account definitions](#) on page 62
- [Default project templates for synchronizing an Oracle E-Business Suite](#) on page 178
- [Entering main data of E-Business Suite user accounts](#) on page 134

# Entering main data of E-Business Suite user accounts

## To create a user account

1. In the Manager, select the **Oracle E-Business Suite > 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 **Oracle E-Business Suite > 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.

## Detailed information about this topic


- [General main data of E-Business Suite user accounts](#) on page 134
- [Login data for E-Business Suite user accounts](#) on page 138

# General main data of E-Business Suite user accounts

On the **General** tab, you enter the following main data:

**Table 33: Additional main data of a user account**

Property	Description
Identity	Identity that uses this user account. <ul style="list-style-type: none"><li>• An identity is already entered if the user account was generated by an account definition.</li><li>• If you are using automatic identity assignment, an associated identity is found and added to the user account when you save the user account.</li><li>• If you create the user account manually, you can select an identity in the drop-down.</li></ul>

Property	Description
No link to an identity required	<p>The drop-down displays activated and deactivated identities by default. If you do not want to see any deactivated identities, set the <b>QER   Person   HideDeactivatedIdentities</b> configuration parameter.</p> <p><b>NOTE:</b> If you assign a deactivated identity to a user account, it might be locked or deleted depending on the configuration.</p> <p>You can create a new identity for a user account with an identity of type <b>Organizational identity, Personalized administrator identity, Sponsored identity, Shared identity, or Service identity</b>. 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.</p>
Not linked to an identity	<p>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).</p> <p>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.</p> <p>Indicates why the <b>No link to an identity required</b> option is enabled for this user account. Possible values:</p> <ul style="list-style-type: none"> <li>• <b>By administrator:</b> The option was set manually by the administrator.</li> <li>• <b>By attestation:</b> The user account was attested.</li> <li>• <b>By exclusion criterion:</b> 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 <b>PersonExcludeList</b>).</li> </ul>
Account definition	<p>Account definition through which the user account was created.</p> <p>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.</p> <p><b>NOTE:</b> The account definition cannot be changed once the user account has been saved.</p> <p><b>NOTE:</b> Use the user account's <b>Remove account definition</b> task to reset the user account to <b>Linked</b> status. This removes the account definition from both the user account and the identity. The user</p>

Property	Description
	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 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.
User name	User account identifier. If you have assigned an account definition, this input field is filled automatically depending on the manage level.
Display name	User account display name. If you have assigned an account definition, this input field is filled automatically depending on the manage level.
Distinguished name	User account's distinguished name. This is formed based on a template from the user name and the distinguished name of the E-Business Suite system.
Email address	User account email address. If you have assigned an account definition, this input field is filled automatically depending on the manage level.
Fax	Fax number for the user account. If you have assigned an account definition, this input field is filled automatically depending on the manage level.
Status	<p>Status of the user account. The status is set using a template. The value depends on the validity period of the user account (<b>Active from (date), Active to (date)</b>).</p> <p>Permitted values are:</p> <ul style="list-style-type: none"> <li>• <b>ACTIVE:</b> The current date is within the validity period.</li> <li>• <b>INACTIVE:</b> The active-from date has not yet been reached or the active-to date is in the past.</li> </ul>
Active from (date)	First date from which the user account is valid. If you have assigned an account definition, this input field is filled automatically depending on the manage level. The template is only effective if the user account has been created as a new user account.
Active to (date)	Last date from which the user account is valid If you have assigned an account definition, this input field is filled automatically depending on the manage level.
E-Business Suite system	E-Business Suite system in which you want to create the user account.
Customer	Reference to an identity that is listed as a customer.

Property	Description
	Only identities from the <b>E-Business Suite AR</b> data source can be assigned ( <code>Person.ImportSource='EBSOIM'</code> ).
HR employee	Reference to an identity in the Oracle E-Business Suite Human Resources module.  Only identities from the <b>E-Business Suite HR</b> data source can be assigned ( <code>Person.ImportSource='EBSHR'</code> ).
Party	Reference to an identity that is listed as a party.  An identity with the <b>E-Business Suite AR</b> data source can be assigned ( <code>Person.ImportSource='EBSOIM'</code> ). The assignment cannot be edited in One Identity Manager.
supplier	Reference to an identity that is listed as a supplier or a contact.  Only identities from the <b>E-Business Suite AP</b> data source can be assigned ( <code>Person.ImportSource='EBSCRM'</code> ).
Risk index (calculated)	Maximum risk index value of all assigned entitlements. The property is only visible if the <b>QER   CalculateRiskIndex</b> configuration parameter is set. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Category	Categories for the inheritance of E-Business Suite permissions to the user account. User accounts can selectively inherit permissions. To do this, entitlements, and user accounts are divided into categories.  Select one or more categories from the drop-down.
Description	Text field for additional explanation.
Identity type	User account's identity type Permitted values are: <ul style="list-style-type: none"> <li>• <b>Primary identity:</b> Identity's default user account.</li> <li>• <b>Organizational identity:</b> Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.</li> <li>• <b>Personalized administrator identity:</b> User account with administrative permissions, used by one identity.</li> <li>• <b>Sponsored identity:</b> User account to use for a specific purpose. Training, for example.</li> <li>• <b>Shared identity:</b> User account with administrative permissions, used by several identities. Assign all identities that use this user account.</li> <li>• <b>Service identity:</b> Service account.</li> </ul>
Privileged user account.	Specifies whether this is a privileged user account.

Property	Description
Entitlements can be inherited	<p>Specifies whether the user account can inherit E-Business Suite permissions through the identity. If this option is set, the user account inherits permissions through hierarchical roles or IT Shop requests. ID</p> <ol style="list-style-type: none"> <li>1. Example: An identity with an E-Business Suite user account is a member of a department. This department is assigned an E-Business Suite entitlement. If this option is set, the user account inherits this entitlement.</li> <li>2. Example: An identity with an E-Business Suite user account requests an E-Business Suite entitlement in the IT Shop. The request is approved and assigned. The user account only inherits this entitlement if this option is active.</li> </ol>
User account is disabled	<p>Specifies whether the user account is blocked from logging in to the E-Business Suite system. The status of the user account is transferred by template. To disable the user account, edit the last validity date of the user account.</p>

## Related topics

- [Managing E-Business Suite user accounts and persons](#) on page 61
- [Setting up account definitions](#) on page 62
- [Assigning identities automatically to E-Business Suite user accounts](#) on page 80
- [Inheritance of E-Business Suite entitlements based on categories](#) on page 125
- [Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts](#) on page 111
- [Disabling E-Business Suite user accounts](#) on page 140
- [Linking E-Business Suite user accounts with imported identities](#) on page 86
- [Supported user account types](#) on page 88

## Login data for E-Business Suite user accounts

On the **Login** tab, enter the password for logging in to the Oracle E-Business Suite. Once you have saved the user account password with One Identity Manager it cannot be changed.

**Table 34: Login data for a user account**

Property	Description
Last login	Date of last login.

Property	Description
Password	<p>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 <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p> <p>If you use a random generated initial password for the user accounts, it is automatically entered when a user account is created.</p> <p>The password is deleted from the database after publishing to the target system.</p> <p><b>NOTE:</b> One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements.</p>
Confirmation	Reconfirm password.
Logins (remaining)	Number of logins remaining until the password expires.
Password last changed	Data of last password change.
Logins	Permitted number of logins.
Days	Validity period for the password.

## Related topics

- [Initial password for new E-Business Suite user accounts](#) on page 106

# Additional tasks for managing E-Business Suite user accounts

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

Task	Topic
Overview of E-Business Suite user accounts	<a href="#">Displaying the E-Business Suite user account overview</a> on page 140
Assigning permissions	<a href="#">Assigning E-Business Suite entitlements directly to a user account</a> on page 118
Assigning extended properties	<a href="#">Assigning extended properties to E-Business Suite user accounts</a> on page 140
Synchronize object	<a href="#">Synchronizing single objects</a> on page 54

## Displaying the E-Business Suite user account overview

### *To obtain an overview of a user account*

1. In the Manager, select the **Oracle E-Business Suite > User accounts** category.
2. Select the user account in the result list.
3. Select the **E-Business Suite user account overview** task.

**TIP:** On the overview form, you can click an assigned security attribute to open the main data form for the assignment. Here you will see the value used to modify this assignment.

## Assigning extended properties to E-Business Suite 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 using 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 **Oracle E-Business Suite > 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.

## Disabling E-Business Suite user accounts

The way you disable 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 disabled 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. For user accounts with a manage level, configure the required behavior using the template in the `EBSUser.EndDate` column.

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

User accounts managed through user account definitions are disabled 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 disabled when the identity is permanently or temporarily disabled.
- If the configuration parameter is not set, the identity's properties do not have any effect on the associated user accounts.

### ***To disable the user account when the configuration parameter is disabled***

1. In the Manager, select the **Oracle E-Business Suite > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. On the **General** tab, enter the current date in the **Active to (date)** input field.  
This sets the status of the user account to **INACTIVE**.
5. Save the changes.

## Scenario: The user accounts are not linked to identities.

### ***To disable a user account that is no longer linked to an identity***

1. In the Manager, select the **Oracle E-Business Suite > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. On the **General** tab, enter the current date in the **Active to (date)** input field.  
This sets the status of the user account to **INACTIVE**.
5. Save the changes.

### ***To activate a user account***

- Delete the last validity date in the **Active to (date)** field.

For more information about deactivating and deleting identities and user accounts, see the *One Identity Manager Target System Base Module Administration Guide*.

## Related topics

- [Setting up account definitions](#) on page 62
- [Creating manage levels](#) on page 65
- [Deleting E-Business Suite user accounts](#) on page 142

# Deleting E-Business Suite user accounts

**NOTE:** 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 disabled. User accounts marked as **Outstanding** will only be deleted if the **QER | Person | User | DeleteOptions | DeleteOutstanding** configuration parameter is set.

E-Business Suite user accounts in One Identity Manager cannot be physically deleted. If a user account is deleted through the result list or the menu bar, the user account is deactivated. However, it still physically exists. After confirmation of the security prompt, the status of the user account is set to **INACTIVE**. The current date is stored as the last validity date of the user account (**Active to (date)**).

## Related topics


- [Disabling E-Business Suite user accounts](#) on page 140

# E-Business Suite permissions

E-Business Suite User accounts are assigned permissions for objects Oracle E-Business Suite by means of responsibilities. Responsibilities cannot be assigned to user accounts directly. Instead, they are inherited by means of security groups. Permissions in Oracle E-Business Suite are characterized by the combination of responsibilities and security groups. These combinations are mapped in the One Identity Manager database as E-Business Suite permissions.

# Entering main data of E-Business Suite entitlements

## To edit the main data of an entitlement:

1. In the Manager, select the **Oracle E-Business Suite > entitlements** category.
2. To edit an entitlement, select the entitlement in the result list and run the **Change main data** task.  
- OR -  
To create a entitlement, click  in the result list.  
This opens the main data form for an E-Business Suite entitlement.
3. Edit the main data of the entitlement.
4. Save the changes.

## Detailed information about this topic

- [General main data of an E-Business Suite entitlement](#) on page 143

# General main data of an E-Business Suite entitlement

For an E-Business Suite entitlement, enter the following main data:

**Table 35: General main data of an entitlement**

Property	Description
E-Business Suite Responsibility	Responsibility for which the entitlement is to be created The responsibility must belong to the same E-Business Suite system as the security group.
Security group	Security group for which the entitlement is to be created. The security group must belong to the same E-Business Suite system as the responsibility.
Display name	Display name for the entitlement
Category	Categories for the inheritance of entitlements to user accounts User accounts can selectively inherit permissions. To do this, entitlements, and user accounts are divided into categories. Select one or more categories from the drop-down.
Risk index	Value for evaluating the risk of assigning the entitlement to user

Property	Description
	accounts. Enter a value between <b>0</b> and <b>1</b> . This field is only visible if the <b>QER   CalculateRiskIndex</b> configuration parameter is set. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Service item	Service item for requesting the entitlement through the IT Shop.
IT Shop	Specifies whether the entitlement can be requested through the IT Shop. This entitlement can be requested by your employees through the Web Portal and allocated by defined approval processes. The entitlement can still be assigned directly to user accounts and hierarchical roles.
Only for use in IT Shop	Specifies whether the entitlement can only be requested through the IT Shop. This entitlement can be requested by your employees through the Web Portal and allocated by defined approval processes. Direct assignment of the entitlement to hierarchical roles or user accounts is not permitted.

## Related topics

- [Inheritance of E-Business Suite entitlements based on categories](#) on page 125
- [Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts](#) on page 111
- [Adding E-Business Suite entitlements to the IT Shop](#) on page 115

## Additional tasks for managing E-Business Suite entitlements

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

Task	Theme
Overview of E-Business Suite entitlements	<a href="#">Displaying E-Business Suite entitlement overviews</a> on page 145
assign user accounts	<a href="#">Assigning E-Business Suite user accounts directly to an entitlement</a> on page 117
Assigning extended properties	<a href="#">Assigning extended properties to E-Business Suite entitlements</a> on page 145
Exclude E-Business Suite entitlements	<a href="#">Effectiveness of entitlement assignments</a> on page 122

Task	Theme
Assign system roles	<a href="#">Adding E-Business Suite entitlements to system roles</a> on page 114
Assign business roles	<a href="#">Assigning E-Business Suite entitlements to business roles</a> on page 113
Assign organizations	<a href="#">Assigning E-Business Suite entitlements to departments, cost centers, and locations</a> on page 112
Add to IT Shop	<a href="#">Adding E-Business Suite entitlements to the IT Shop</a> on page 115
Synchronize object	<a href="#">Synchronizing single objects</a> on page 54

## Displaying E-Business Suite entitlement overviews

### *To obtain an overview of permissions*

1. In the Manager, select the **Oracle E-Business Suite > entitlements** category.
2. Select the entitlements in the result list.
3. Select the **E-Business Suite entitlements overview** task.

## Assigning extended properties to E-Business Suite entitlements

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 using extended properties, see the *One Identity Manager Compliance Rules Administration Guide*.

### *To specify extended properties for an entitlement*

1. In the Manager, select the **Oracle E-Business Suite > entitlements** category.
2. Select the E-Business Suite entitlement in the result list.
3. Select **Assign extended properties**.
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.

## E-Business Suite applications

The applications integrated in E-Business Suite are mapped based on Oracle E-Business Suite applications. Applications are imported into the One Identity Manager database during synchronization. You cannot edit the properties.

### **To display the properties of an application:**

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Applications** category.
2. Select the application in the result list.
3. Select the **Change main data** task.

The overview form displays the relationships of an application to E-Business Suite groups and responsibilities.

### **To obtain an overview of an application:**

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Applications** category.
2. Select the application in the result list.
3. Select the **E-Business Suite application overview** task.

### **Related topics**

- [Synchronizing single objects](#) on page 54

## E-Business Suite menus

The linking of a user account to a menu is an important part of access control in Oracle E-Business Suite. Menus are imported into the One Identity Manager database during synchronization. You cannot edit the properties.

### **To display the properties of a menu:**

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Menus** category.

2. Select the menu in the result list.
3. Select the **Change main data** task.

Menus are assigned to user accounts through E-Business Suite responsibilities. Each responsibility can reference only one menu. This relationship is displayed on the overview form for a menu.

**To view an overview of a menu:**

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Menus** category.
2. Select the menu in the result list.
3. Select the **E-Business Suite menu overview** task.

**Related topics**

- [Synchronizing single objects](#) on page 54

## E-Business Suite data groups

E-Business Suite data groups are used to control how different user accounts access tables in the Oracle E-Business Suite data. Data groups define which tables belong to an E-Business Suite application. User accounts are granted their permissions to these tables through the assignment to E-Business Suite responsibilities. Data groups are imported into the One Identity Manager database during synchronization. You cannot edit the properties.

**To display the properties of a data group:**

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Data groups** category.
2. Select the data group in the result list.
3. Select the **Change main data** task.

**To obtain an overview of a data group:**

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Data groups** category.
2. Select the data group in the result list.
3. Select the **E-Business Suite data group overview** task.

**Related topics**

- [Synchronizing single objects](#) on page 54

# E-Business Suite data group units

E-Business Suite data group units contain data groups that are assigned to E-Business Suite applications. This enables data groups approved for an application to be assigned to E-Business Suite responsibilities. Data group units are loaded into the One Identity Manager database during synchronization. You cannot edit the assignments.

## *To display the properties of a data group unit:*

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Applications > <Application> > Data group units** category.
2. Select the data group unit in the result list.
3. Select **Change main data**.

## *To obtain an overview of a data group unit:*

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Applications > <Application> > Data group units** category.
2. Select the data group unit in the result list.
3. Select the **E-Business Suite data group unit overview** task.

## Related topics

- [Synchronizing single objects](#) on page 54

# E-Business Suite request groups

E-Business Suite request groups can be used to assign permissions for running programs and functions. Request groups are assigned to E-Business Suite applications. They are imported into the One Identity Manager database during synchronization. You cannot edit the properties.

## *To display the properties of a request group:*

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Applications > <Application> > Request groups** category.
2. Select the request group in the result list.
3. Select the **Change main data** task.

### ***To obtain an overview of a request group:***

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Applications > <Application> > Request groups** category.
2. Select the request group in the result list.
3. Select the **E-Business Suite request group overview** task.

### **Related topics**

- [Synchronizing single objects](#) on page 54

## **E-Business Suite security groups**

You use E-Business Suite security groups to further restrict the responsibilities of user accounts. Security groups are imported into the One Identity Manager database during synchronization. You cannot edit the properties.

### ***To display the properties of a security group:***

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Security groups** category.
2. Select the security group in the result list.
3. Select the **Change main data** task.

### ***To obtain an overview of a security group:***

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Security groups** category.
2. Select the security group in the result list.
3. Select the **E-Business Suite security group overview** task.

### **Related topics**

- [Synchronizing single objects](#) on page 54

## **E-Business Suite attributes**

E-Business Suite Attributes further restrict the responsibilities of user accounts. For this purpose, attributes can be assigned both to user accounts and to responsibilities. Attributes are defined for each E-Business Suite application. They are imported into the One Identity Manager database during synchronization. You cannot edit the properties.

### ***To display the properties of an attribute:***

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Applications > <Application> > Attributes** category.
2. Select the attribute in the result list.
3. Select the **Change main data** task.

Attributes that are assigned to user accounts or responsibilities are called security attributes. They can be modified by additional values. These relationships are displayed on the overview form for an attribute.

### ***To view an overview of an attribute***

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Applications > <Application> > Attributes** category.
2. Select the attribute in the result list.
3. Select the **E-Business Suite attribute overview** task.

On the overview form for an attribute, click an assigned user account or an assigned responsibility to open the main data form for the assignment. Here you will see the value used to modify this assignment.

### **Related topics**

- [Synchronizing single objects](#) on page 54

## **E-Business Suite responsibilities**

E-Business Suite responsibilities control the access permissions of a user account in Oracle E-Business Suite. Responsibilities refer to one specific version. E-Business Suite responsibilities are imported into the One Identity Manager database by the synchronization. You cannot edit the properties.

E-Business Suite attributes further restrict the responsibilities. Lists of security attributes and exclusion attributes can be defined. Sub-menus can be explicitly excluded from the assignment to a responsibility. These relationships are displayed on the overview form.

### **Related topics**

- [Synchronizing single objects](#) on page 54

# Displaying main data of E-Business Suite responsibilities

## *To display the properties of a responsibility:*

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Applications > <Application> > Responsibilities** category.
2. Select the responsibility in the result list.
3. Select **Change main data**.

## *To obtain an overview of a responsibility:*

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite system> > Applications > <Application> > Responsibilities** category.
2. Select the responsibility in the result list.
3. Select the **E-Business Suite responsibility overview** task.

On the overview form for a responsibility, you can click an assigned security attribute to open the main data form for the assignment. Here you will see the value used to modify this assignment.

## Detailed information about this topic

- [General main data of E-Business Suite responsibilities](#) on page 151

# General main data of E-Business Suite responsibilities

For E-Business Suite responsibilities, the following properties are mapped.

**Table 36: General main data of a responsibility**

Property	Description
Identifier	Unique identifier of the responsibility in E-Business Suite.
Responsibility key	Description of the responsibility. The responsibility key is unique for each application.
Responsibility name	Display name of the responsibility.
Valid from	First date on which the responsibility is valid.

Property	Description
(date)	
Valid to (date)	Last date on which the responsibility is valid When this date has passed, the responsibility is deactivated.
Description	Additional information about the responsibility.
Language	Language code of the language in which the responsibility is saved in Oracle E-Business Suite.
Application	Application in which the responsibility is valid.
Data group unit	Data group unit for which the responsibility applies.
Menu	Menu for which the responsibility applies
Process group	Request group for which the responsibility applies.
Version	Version in which the responsibility is available Possible value are: <ul style="list-style-type: none"> <li>• AOL (Oracle Applications)</li> <li>• Web (Oracle Self-Service Web Applications)</li> <li>• Mobile (Oracle Mobile Applications)</li> <li>• Direct Access</li> <li>• None</li> </ul>
Web Host Name	IP address or name of the web server.
Web Agent Name	Name of the web agent that specifies the database.
Terminal permissions	Specifies whether terminal permissions are approved for the responsibility.

## HR people

HR people are all persons imported from the table HR.PER\_ALL\_PEOPLE\_F of Oracle E-Business Suite. These persons can be assigned to E-Business Suite user accounts as HR people. The managers of the HR people are also imported.

### ***To display the properties of an HR person:***

1. In the Manager, select the **Oracle E-Business Suite > HR people** category.
2. Select the HR person in the result list.
3. Select the **Change main data** task.

On the **More** tab, the **Import data source** property is displayed with the value **E-Business Suite HR**.

4. Select the **Identity overview** task.

The overview form displays the user accounts to which the identity is assigned as an HR person.

The main data of the imported identities can only be edited to a limited extent in One Identity Manager because Oracle E-Business Suite is the primary system for certain properties.

The following identity main data is locked and cannot be edited:

- First name
- Last name
- Form of address
- Middle name
- Name at birth
- Date of birth
- Entry date
- Manager
- Primary location

You can maintain all other main data in the usual way. For more information about editing identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

**NOTE:** Identities who were imported from Oracle E-Business Suite cannot be deleted in One Identity Manager.

## Related topics

- [Linking E-Business Suite user accounts with imported identities](#) on page 86
- [General main data of E-Business Suite user accounts](#) on page 134
- [Setting up a synchronization project for identity data](#) on page 27
- [Project template for HR data](#) on page 179

# Suppliers and contacts

Suppliers and contacts are all persons imported from the table AP.AP\_SUPPLIER\_CONTACTS of Oracle E-Business Suite. These persons can be assigned as suppliers to E-Business Suite user accounts.

### **To display the properties of a supplier:**

1. In the Manager, select the **Oracle E-Business Suite > Suppliers and contacts** category.
2. Select the identity in the result list.
3. Select the **Change main data** task.

On the **More** tab, the **Import data source** property is displayed with the **E-Business Suite AP** value.

4. Select the **Identity overview** task.

The overview form displays the user accounts to which the identity is assigned as a supplier.

The main data of the imported identities can only be edited to a limited extent in One Identity Manager because Oracle E-Business Suite is the primary system for certain properties.

The following identity main data is locked and cannot be edited:

- First name
- Last name
- Form of address
- Middle name
- Title
- Default email address
- Phone

You can maintain all other main data in the usual way. For more information about editing identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

**NOTE:** Identities who were imported from Oracle E-Business Suite cannot be deleted in One Identity Manager.

### **Related topics**

- [Linking E-Business Suite user accounts with imported identities](#) on page 86
- [General main data of E-Business Suite user accounts](#) on page 134
- [Setting up a synchronization project for organizational data](#) on page 28
- [Project template for CRM data](#) on page 180

## **Parties**

Parties are all persons imported from the table AR.HZ\_PARTIES in Oracle E-Business Suite. These persons can be assigned as customers to E-Business Suite user accounts. The

assignment as a party can only be imported into the One Identity Manager database through the synchronization.

**To display the properties of a party:**

1. In the Manager, select the **Oracle E-Business Suite > Parties** category.
2. Select the identity in the result list.
3. Select the **Change main data** task.

On the **More** tab, the property **Import data source** is displayed with the value **E-Business Suite AR**.

4. Select the **Identity overview** task.

The overview form displays the user accounts to which the identity is assigned as a party or customer.

The main data of the imported identities can only be edited to a limited extent in One Identity Manager because Oracle E-Business Suite is the primary system for certain properties.

The following identity main data is locked and cannot be edited:

- First name
- Last name
- Form of address
- City
- Zip code
- Street
- Country
- State

You can maintain all other main data in the usual way. For more information about editing identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

**NOTE:** Identities who were imported from Oracle E-Business Suite cannot be deleted in One Identity Manager.

## Related topics

- [Linking E-Business Suite user accounts with imported identities](#) on page 86
- [General main data of E-Business Suite user accounts](#) on page 134
- [Setting up a synchronization project for organizational data](#) on page 28
- [Project template for OIM data](#) on page 180

# Locations

During synchronization of data from the Oracle E-Business Suite Human Resources module, location data and the assignments of identities to locations are also imported in addition to the identity data. The locations are mapped using the **E-Business Suite HR** data source.

## **To display locations that originate from the HR data import:**

- In the Manager, select the **Organizations > Locations > Data source > E-Business Suite HR** category.

The main data of the imported locations can only be edited to a limited extent in One Identity Manager, because Oracle E-Business Suite is the master system for certain properties.

To edit locked main data:

- Location
- Description
- Street
- City
- Country

You can maintain all other main data in the usual way. For more information about editing locations, see the *One Identity Manager Identity Management Base Module Administration Guide*.

**NOTE:** Locations who were imported from Oracle E-Business Suite cannot be deleted in One Identity Manager.

## **Related topics**

- [Setting up a synchronization project for identity data](#) on page 27
- [Project template for HR data](#) on page 179

# Departments

During synchronization of data from the Oracle E-Business Suite's Human Resources module, department, and identity departments assignments are loaded as well as the identity data. The departments are displayed with the data source import **E-Business Suite HR**.

### To display departments that come from importing HR data

- In the Manager, select the **Organizations > Departments > Data source > E-Business Suite HR** category.

For more information about editing departments, see the *One Identity Manager Identity Management Base Module Administration Guide*.

**NOTE:** Departments that have been imported from Oracle E-Business Suite cannot be deleted in One Identity Manager.

### Related topics

- [Setting up a synchronization project for identity data](#) on page 27
- [Project template for HR data](#) on page 179
- [Configuring department synchronization](#) on page 36

## Reports about E-Business Suite 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 E-Business Suite systems.

**Table 37: 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 ( <b>Min. date</b> ). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	Entitlement	This report finds all roles containing identities who have the selected system entitlement.
Show overview	Entitlement	This report shows an overview of the system entitlement and its assignments.
Show overview including origin	Entitlement	This report shows an overview of the system entitlement and origin of the assigned user

Report	Published for	Description
		accounts.
Show overview including history	Entitlement	This report shows an overview of the system entitlement and including its history. Select the end date for displaying the history ( <b>Min. date</b> ). Older changes and assignments that were removed before this date, are not shown in the report.
Show entitlement drifts	system	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)	System	This report returns all the user accounts with their permissions including a history. Select the end date for displaying the history ( <b>Min. date</b> ). 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	system	This report contains all user accounts with an above average number of system entitlements.
Show system entitlements overview (incl. history)	system	This report shows the system entitlements with the assigned user accounts including a history. Select the end date for displaying the history ( <b>Min. date</b> ). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	system	This report finds all roles containing identities with at least one user account in the selected target system.
Show unused user accounts	system	This report contains all user accounts, which have not been used in the last few months.

**Table 38: Additional reports for the target system**

Report	Description
E-Business Suite user account and permission assignment	This report contains a summary of user account and permission assignment in all E-Business Suite systems. You can find the report in the <b>My One Identity Manager &gt; Target system overviews</b> category.

<b>Report</b>	<b>Description</b>
Data quality summary for E-Business Suite user accounts	This report contains different evaluations of user account data quality in all E-Business Suite systems. You can find the report in the <b>My One Identity Manager &gt; Data quality analysis</b> category.

## Handling of E-Business Suite objects in the Web Portal

One Identity Manager enables its users to perform various tasks simply using a Web Portal.

- Managing user accounts and identities

An account definition can be requested by shop customers in the Web Portal if it is assigned to an IT Shop shelf. The request undergoes a defined approval process. The user account is not created until it has been agreed by an authorized identity, such as a manager.

- Managing entitlement assignments

When an entitlement is assigned to an E-Business Suite shelf, the IT Shop entitlement can be requested by the customer in the Web Portal. The request undergoes a defined approval process. The entitlement is not assigned until it has been approved by an authorized identity.

In the Web Portal, managers and administrators of organizations can assign E-Business Suite entitlements to the departments, cost centers, or locations for which they are responsible. The entitlements are inherited by all persons who are members of these departments, cost centers, or locations.

If the Business Roles Module is available, managers and administrators of business roles in the Web Portal can assign E-Business Suite entitlements to the business roles for which they are responsible. The entitlements are inherited by all persons who are members of these business roles.

If the System Roles Module is available, supervisors of system roles in the Web Portal can assign E-Business Suite entitlements to the system roles. The entitlements are inherited by all persons to whom these system roles are assigned.

- Attestation

If the Attestation Module is available, the correctness of the properties of target system objects and of entitlement assignments can be verified on request. To enable this, attestation policies are configured in the Manager. The attestors use the Web Portal to approve attestation cases.

- Governance administration

If the Compliance Rules Module is available, you can define rules that identify the invalid entitlement assignments and evaluate their risks. The rules are checked regularly, and if changes are made to the objects in One Identity Manager. Compliance rules are defined in the Manager. Supervisors use the Web Portal to check rule violations and to grant exception approvals.

If the Company Policies Module is available, company policies can be defined for the target system objects mapped in One Identity Manager and their risks evaluated. Company policies are defined in the Manager. Supervisors use the Web Portal to check policy violations and to grant exception approvals.

- Risk assessment

You can use the risk index of E-Business Suite entitlements to evaluate the risk of entitlement assignments for the company. One Identity Manager provides default calculation functions for this. The calculation functions can be modified in the Web Portal.

- Reports and statistics

The Web Portal provides a range of reports and statistics about the identities, user accounts, and their entitlements and risks.

For more information about the named topics, see [Assigning E-Business Suite entitlements to user accounts in One Identity Manager](#) on page 110 and refer to the following guides:

- One Identity Manager Web Portal User Guide
- One Identity Manager Attestation Administration Guide
- One Identity Manager Compliance Rules Administration Guide
- One Identity Manager Company Policies Administration Guide
- One Identity Manager Risk Assessment Administration Guide

## Basic configuration data

To manage Oracle E-Business Suite in One Identity Manager, the following data is relevant.

- 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 62.

- 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 policies 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 E-Business Suite user accounts](#) on page 95.

- 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 55.

- 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 [Job server for E-Business Suite-specific process handling](#) on page 163.

- 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 E-Business Suite systems in One Identity Manager.

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

For more information, see [Target system managers](#) on page 168.

## Job server for E-Business Suite-specific process handling

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*.
- In the Manager, select an entry for the Job server in the **Oracle E-Business Suite > Basic configuration data > Server** category and edit the Job server's 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*.

### Related topics

- [System requirements for the synchronization server](#) on page 17

## Editing E-Business Suite Job servers

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.

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

1. In the Manager, select the **Oracle E-Business Suite > 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

- [General main data of Job servers](#) on page 164
- [Specifying server functions](#) on page 167

## General main data of Job servers

**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 39: Job server properties**

Property	Meaning
Server	Job server name.
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. <b>NOTE:</b> The <b>Server is cluster</b> and <b>Server belongs to cluster</b> 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

Property	Meaning
	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 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 <b>win32</b> , <b>Windows</b> , <b>Linux</b> , and <b>Unix</b> are permitted. If no value is specified, <b>win32</b> 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

Property	Meaning
	<p>installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure the moment the queue is called for the first time.</p> <p>The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.</p>
Stop One Identity Manager Service	<p>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.</p> <p>You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more information, see the <i>One Identity Manager Process Monitoring and Troubleshooting Guide</i>.</p>
Paused due to unavailability of a target system	<p>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.</p> <p>For more information about offline mode, see the <i>One Identity Manager Target System Synchronization Reference Guide</i>.</p>
No automatic software update	<p>Specifies whether to exclude the server from automatic software updating.</p> <p><b>NOTE:</b> Servers must be manually updated if this option is set.</p>
Software update running	<p>Specifies whether a software update is currently running.</p>
Server function	<p>Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.</p>

## Related topics

- [Specifying server functions](#) on page 167

# 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 40: Permitted server functions**

Server function	Remark
Update server	<p>This server automatically updates the software on all 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.</p> <p>The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.</p>
SQL processing server	<p>It can run SQL tasks. The server requires a direct connection to the database server that One Identity Manager database is installed on.</p> <p>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.</p>
CSV script server	<p>This server can process CSV files using the ScriptComponent process component.</p>
One Identity Manager Service installed	<p>Server on which a One Identity Manager Service is installed.</p>
SMTP host	<p>Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.</p>
Default report server	<p>Server on which reports are generated.</p>
Oracle E-Business Suite connector	<p>Server on which the Oracle E-Business Suite connector is installed. This server synchronizes the Oracle E-Business Suite target system.</p>

## Related topics

- [General main data of Job servers](#) on page 164

# 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 E-Business Suite systems in One Identity Manager.

Define additional application roles if you want to limit the permissions for target system managers to individual systems. 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 E-Business Suite systems 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 E-Business Suite systems.

**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 41: Default application roles for target system managers**

User	Tasks
Target system managers	<p>Target system managers must be assigned to the <b>Target systems   Oracle E-Business Suite</b> or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"><li>• Assume administrative tasks for the target system.</li><li>• Create, change, or delete target system objects.</li><li>• Edit password policies for the target system.</li><li>• Prepare entitlements to add to the IT Shop.</li><li>• Can add identities that do not have the <b>Primary identity</b> identity type.</li><li>• Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.</li></ul>

User	Tasks
	<ul style="list-style-type: none"> <li>• Edit the synchronization's target system types and outstanding objects.</li> <li>• Authorize other identities within their area of responsibility as target system managers and create child application roles if required.</li> </ul>

### ***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 > Oracle E-Business Suite** 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 **Oracle E-Business Suite > 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 E-Business Suite systems***

1. Log in to the Manager as a target system manager.
2. Select the **Oracle E-Business Suite > Systems** category.
3. Select the system 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 | Oracle E-Business Suite** 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 system in One Identity Manager.

## Related topics

- [One Identity Manager users for managing Oracle E-Business Suite](#) on page 10
- [General main data of E-Business Suite systems](#) on page 130

## Configuration parameters for managing Oracle E-Business Suite

The following configuration parameters are additionally available in One Identity Manager after the module has been installed.

**Table 42: Configuration parameters**

Configuration parameter	Meaning
TargetSystem   EBS	<p>Preprocessor relevant configuration parameter for controlling database model components for Oracle E-Business Suite target system administration. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.</p> <p>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 <i>One Identity Manager Configuration Guide</i>.</p>
TargetSystem   EBS   Accounts	Parameter for configuring E-Business Suite user account data.
TargetSystem   EBS   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   EBS   Accounts   InitialRandomPassword   SendTo	Specifies to which identity the email with the random generated password should be sent (manager cost center-/department/location/role, identity's manager or XUserInserted). If no recipient can be found, the email is sent to the address stored in the configuration parameter <b>TargetSystem   EBS   DefaultAddress</b> .
TargetSystem   EBS	Mail template name that is sent to supply users with the login

Configuration parameter	Meaning
Accounts   InitialRandomPassword   SendTo   MailTemplateAccountName	credentials for the user account. The <b>Identity - new user account created</b> mail template is used.
TargetSystem   EBS   Accounts   InitialRandomPassword   SendTo   MailTemplatePassword	Mail template name that is sent to supply users with the initial password. The <b>Identity - initial password for new user account</b> mail template is used.
TargetSystem   EBS   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 <b>Identity - new user account with default properties created</b> mail template is used.
TargetSystem   EBS   Accounts   PrivilegedAccount	Allows configuration of privileged user account settings.
TargetSystem   EBS   Accounts   PrivilegedAccount   AccountName_Postfix	Postfix for formatting the login name of privileged user accounts.
TargetSystem   EBS   Accounts   PrivilegedAccount   AccountName_Prefix	Prefix for formatting a login name of privileged user accounts.
TargetSystem   EBS   DefaultAddress	Default email address of the recipient for notifications about actions in the target system.
TargetSystem   EBS   MaxFullsyncDuration	Maximum runtime of a synchronization in minutes. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem   EBS   PersonAutoDefault	Mode for automatic identity assignment for user accounts added to the database outside synchronization.
TargetSystem   EBS   PersonAutoDisabledAccounts	Specifies whether identities are automatically assigned to disabled user accounts. User accounts are not given an account definition.
TargetSystem   EBS   PersonAutoFullsync	Mode for automatic identity assignment for user accounts that are added to or updated in the database by synchronization.

Configuration parameter	Meaning
TargetSystem   EBS   PersonExcludeList	<p>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.</p> <p>Example:</p> <pre>ADMINISTRATOR GUEST KRBTGT TSINTERNETUSER IUSR_.* IWAM_.*  SUPPORT_.* . *   \$</pre>

The following configuration parameters are also required.

**Table 43: Additional configuration parameters**

Configuration parameter	Meaning
Common   Journal   Delete   BulkCount	Number of entries to be deleted in any operation.
Common   Journal   Delete   TotalCount	Total number of entries to be deleted in any processing run.
Common   Journal   LifeTime	Use this configuration parameter to specify the maximum amount of time (in days) that a system journal entry can be stored in the database. Older entries are deleted from the database.
Common   MailNotification   DefaultSender	<p>Sender's default email address for sending automatically generated notifications.</p> <p>Syntax:</p> <pre>sender@company.com</pre> <p>Example:</p> <pre>noreply@company.com</pre> <p>You can enter the sender's display name in addition to the email address. In this case, ensure that the email address is enclosed in chevrons (&lt;&gt;).</p> <p>Example:</p> <pre>One Identity &lt;noreply@company.com&gt;</pre>
DPR   Journal   LifeTime	This configuration parameter specifies the synchronization log's retention period (in days). Older logs are deleted from the database.
QER   CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating the risk index. Changes to the parameter require recompiling the database.

Configuration parameter	Meaning
QER   Person   TemporaryDeactivation	<p>If the parameter is enabled, values for the risk index can be entered and calculated.</p> <p>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 <i>One Identity Manager Configuration Guide</i>.</p>
QER   Person   UseCentralPassword	<p>This configuration parameter specifies whether user accounts for an identity are locked if the identity is temporarily or permanently disabled.</p>
QER   Structures   Inherit   GroupExclusion	<p>Specifies whether the identity's central password is used in the user accounts. The identity's central password is automatically mapped to the identity's user accounts in all permitted target systems. This excludes privileged user accounts, which are not updated.</p>
QER   Structures   Inherit   GroupExclusion	<p>Preprocessor-relevant configuration parameter for controlling the effectiveness of permissions. If this parameter is set, the assigned permissions can be reduced based on exclusion definitions. Changes to this parameter require the database to be recompiled.</p>

## Permissions required for synchronizing with Oracle E-Business Suite

The Oracle E-Business Suite requires read access rights to at least the following database objects in the Oracle Database to be connected.

**Table 44: Tables and views with select entitlements**

Tables	Views
<ul style="list-style-type: none"><li>• ak.ak_attributes_tl</li></ul>	<ul style="list-style-type: none"><li>• ak.ak_attributes_tl#</li></ul>
<ul style="list-style-type: none"><li>• ak.ak_excluded_items</li></ul>	<ul style="list-style-type: none"><li>• ak.ak_excluded_items#</li></ul>
<ul style="list-style-type: none"><li>• ak.ak_resp_security_attr_values</li></ul>	<ul style="list-style-type: none"><li>• ak.ak_resp_security_attr_values#</li></ul>
<ul style="list-style-type: none"><li>• ak.ak_web_user_sec_attr_values</li></ul>	<ul style="list-style-type: none"><li>• ak.ak_web_user_sec_attr_values#</li></ul>
<ul style="list-style-type: none"><li>• applsys.fnd_application</li></ul>	<ul style="list-style-type: none"><li>• applsys.fnd_application#</li></ul>
<ul style="list-style-type: none"><li>• applsys.fnd_application_tl</li></ul>	<ul style="list-style-type: none"><li>• applsys.fnd_application_tl#</li></ul>
<ul style="list-style-type: none"><li>• applsys.fnd_data_groups</li></ul>	<ul style="list-style-type: none"><li>• applsys.fnd_data_groups#</li></ul>
<ul style="list-style-type: none"><li>• applsys.fnd_data_group_units</li></ul>	<ul style="list-style-type: none"><li>• applsys.fnd_data_group_units#</li></ul>
<ul style="list-style-type: none"><li>• applsys.fnd_languages</li></ul>	<ul style="list-style-type: none"><li>• applsys.fnd_languages#</li></ul>
<ul style="list-style-type: none"><li>• applsys.fnd_menus</li></ul>	<ul style="list-style-type: none"><li>• applsys.fnd_menus#</li></ul>
<ul style="list-style-type: none"><li>• applsys.fnd_menus_tl</li></ul>	<ul style="list-style-type: none"><li>• applsys.fnd_menus_tl#</li></ul>
<ul style="list-style-type: none"><li>• applsys.fnd_profile_options</li></ul>	<ul style="list-style-type: none"><li>• applsys.fnd_request_groups#</li></ul>
<ul style="list-style-type: none"><li>• applsys.fnd_profile_option_values</li></ul>	<ul style="list-style-type: none"><li>• applsys.fnd_responsibility#</li></ul>
<ul style="list-style-type: none"><li>• applsys.fnd_request_groups</li></ul>	<ul style="list-style-type: none"><li>• applsys.fnd_responsibility_tl#</li></ul>
<ul style="list-style-type: none"><li>• applsys.fnd_resp_functions</li></ul>	<ul style="list-style-type: none"><li>• applsys.fnd_security_groups#</li></ul>
<ul style="list-style-type: none"><li>• applsys.fnd_responsibility</li></ul>	<ul style="list-style-type: none"><li>• applsys.fnd_security_groups_tl#</li></ul>
<ul style="list-style-type: none"><li>• applsys.fnd_responsibility_tl</li></ul>	<ul style="list-style-type: none"><li>• applsys.fnd_user#</li></ul>
<ul style="list-style-type: none"><li>• applsys.fnd_security_groups</li></ul>	

**Tables****Views**

- applsys.fnd\_security\_groups\_tl
- applsys.fnd\_user
- apps.fnd\_user\_resp\_groups\_all
- apps.fnd\_user\_resp\_groups\_direct
- apps.fnd\_user\_resp\_groups\_indirect
- apps.fnd\_usr\_roles

**Table 45: Stored procedures with run permissions****Stored procedures**

- apps.fnd\_preference  
This grants permissions for the following procedures.
  - apps.fnd\_preference.put
  - apps.fnd\_preference.remove
- apps.fnd\_user\_pkg  
This grants permissions for the following procedures.
  - apps.fnd\_user\_pkg.AddResp
  - apps.fnd\_user\_pkg.change\_user\_name
  - apps.fnd\_user\_pkg.changepassword
  - apps.fnd\_user\_pkg.CreateUser
  - apps.fnd\_user\_pkg.DelResp
  - apps.fnd\_user\_pkg.DisableUser
  - apps.fnd\_user\_pkg.UpdateUser
  - apps.fnd\_user\_pkg.user\_synch

**Table 46: Tables with select permissions for synchronizing identity data****Tables****Views**

- |                                |                                  |
|--------------------------------|----------------------------------|
| • ap.ap_supplier_contacts      | • hr.hr_all_organization_units#  |
| • ar.hz_parties                | • hr.hr_locations_all#           |
| • hr.hr_all_organization_units | • hr.per_all_assignments_f#      |
| • hr.hr_locations_all          | • hr.per_all_people_f#           |
| • hr.per_all_assignments_f     | • hr.per_job_groups#             |
| • hr.per_all_people_f          | • hr.per_jobs#                   |
| • hr.per_job_groups            | • hr.per_org_structure_versions# |

**Tables**

- hr.per\_jobs
- hr.per\_org\_structure\_versions
- hr.per\_org\_structure\_elements
- hr.per\_roles
- hr.per\_sec\_profile\_assignments
- hr.per\_security\_profiles

**Views**

- hr.per\_org\_structure\_elements#
- hr.per\_sec\_profile\_assignments#
- hr.per\_security\_profiles#

**Table 47: Tables with run permissions for synchronizing identity data****Tables**

- apps.per\_sec\_profile\_asg\_api

**Table 48: Tables with select entitlements for schema types that are created in the connector schema, but are not contained in the default mapping****Tables**

- applsys.fnd\_request\_group\_units
- applsys.fnd\_request\_sets
- applsys.fnd\_request\_sets\_tl
- applsys.fnd\_user\_preferences

**Views**

- applsys.fnd\_request\_group\_units#
- applsys.fnd\_request\_sets#
- applsys.fnd\_user\_preferences#

## Default project templates for synchronizing an Oracle E-Business Suite

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 user accounts and entitlements](#) on page 178
- [Project template for HR data](#) on page 179
- [Project template for CRM data](#) on page 180
- [Project template for OIM data](#) on page 180

## Project template for user accounts and entitlements

To synchronize Oracle E-Business Suite user accounts and permissions, you use the **Oracle E-Business Suite synchronization** project template. The project template uses mappings for the following schema types.

**Table 49: Mapping E-Business Suite schema types to tables in the One Identity Manager schema.**

Schema type in the target system	Table in the One Identity Manager Schema
ORA-Account	EBSUser
ORA-Application	EBSApplication
ORA-Attribute	EBSAttribute
ORA-Datagroup	EBSDataGroup
ORA-Datagroupunit	EBSDataGroupUnit
ORA-Language	EBSLanguage
ORA-Menu	EBSMenu
ORA-Requestgroup	EBSRequestGroup
ORA-RESP	EBSResp
ORA-Responsibility	EBSResponsibility
ORA-ResponsiExcludesAttribute	EBSResponsiExcludesAttribute
ORA-ResponsiExcludesMenu	EBSResponsiExcludesMenu
ORA-ResponsiHasAttribute	EBSResponsiHasAttribute
ORA-Securitygroup	EBSSecurityGroup
ORA-UserHasAttribute	EBSUserHasAttribute
UserInRespDirect	EBSUserInResp
UserInRespIndirect	EBSUserInResp

## Project template for HR data

To synchronize HR people from the Human Resources module of an Oracle E-Business Suite, you use the **Oracle E-Business Suite HR Data** project template. The project template uses mappings for the following schema types.

**Table 50: Mapping E-Business Suite schema types to tables in the One Identity Manager schema.**

Schema type in the target system	Table in the One Identity Manager Schema
HRPerson	Person
HRPersonManager	Person

Schema type in the target system	Table in the One Identity Manager Schema
HRLocations	Locality
HRPersonSecondaryLocation	PersonInLocality
HRPersonPrimaryLocation	Person
HROrganization	Department
HRPersonInOrganization	PersonInDepartment

## Project template for CRM data

For the synchronization of supplier contact data of an Oracle E-Business Suite, you use the project template **Oracle E-Business Suite CRM data**. The project template uses mappings for the following schema types.

**Table 51: Mapping E-Business Suite schema types to tables in the One Identity Manager schema.**

Schema type in the target system	Table in the One Identity Manager Schema
APSupplierContacts	Person

## Project template for OIM data

For the synchronization of party data of an Oracle E-Business Suite, you use the project template **Oracle E-Business Suite OIM data**. The project template uses mappings for the following schema types.

**Table 52: Mapping E-Business Suite schema types to tables in the One Identity Manager schema.**

Schema type in the target system	Table in the One Identity Manager Schema
HZParty	Person

## Editing system objects

The following table describes permitted editing methods for Oracle E-Business Suite schema types.

**Table 53: Methods available for editing schema types**

Schema type	Read	Paste	Delete	Refresh
Application (ORA-Application)	Yes	No	No	No
Attribute (ORA-Attribute)	Yes	No	No	No
Language (ORA-Language)	Yes	No	No	No
Menu (ORA-Menu)	Yes	No	No	No
User accounts (ORA-Account)	Yes	Yes	No	Yes
Data group (ORA-Datagroup)	Yes	No	No	No
Data group unit (ORA-Datagroupunit)	Yes	No	No	No
Request group (ORA-Requestgroup)	Yes	No	No	No
Security group (ORA-SecurityGroup)	Yes	No	No	No
User account: assignment to security attribute (ORA-UserHasAttribute)	Yes	No	No	No
Responsibility/security combi (ORA-RESP)	Yes	No	No	No
Responsibility (ORA-Responsibility)	Yes	No	No	No
Responsibility: exclusion attribute (ORA-ResponsiExcludesAttribute)	Yes	No	No	No
Responsibility: excluded menu (ORA-ResponsiExcludesMenu)	Yes	No	No	No
Responsibility: assigned security attribute (ORA-ResponsiHasAttribute)	Yes	No	No	No
User account: assignment to responsibility (ORA-UserInRESPDirect)	Yes	Yes	No	Yes

<b>Schema type</b>	<b>Read</b>	<b>Paste</b>	<b>Delete</b>	<b>Refresh</b>
User account: assignment to responsibility (ORA-UserInRESPIndirect)	Yes	No	No	No
Identity (APSupplierContacts)	Yes	No	No	No
Identity (HZParty)	Yes	No	No	No
Identity (HRPerson)	Yes	No	No	No
Identity (HRPersonManager)	Yes	No	No	No
Location (HRLocations)	Yes	No	No	No
Secondary assignment: location (HRPersonSecondaryLocation)	Yes	No	No	No
Department (HROrganization)	Yes	No	No	No
Secondary assignment: department (HRPersonInOrganization)	Yes	No	No	No

## Example of a schema extension file

```
<?xml version="1.0" encoding="utf-8" ?>
<EBSF12>
<ObjectNames>
<Object SchemaName="UserInRESPDirect" ParentSchemaName="ORA-RESPDirect"
DisplayPattern="%vrtDistinguishedName%" IsReadOnly="false" UseDistinct="false">
  <ObjectKey>
    <Key Column="APPS.FND_USER_RESP_GROUPS_DIRECT.USER_ID" IsDNCColumn="true"
X500Abbreviation="UR" />
    <Key Column="APPS.FND_USER_RESP_GROUPS_DIRECT.RESPONSIBILITY_ID" />
    <Key Column="APPS.FND_USER_RESP_GROUPS_DIRECT.RESPONSIBILITY_
APPLICATION_ID" />
    <Key Column="APPS.FND_USER_RESP_GROUPS_DIRECT.SECURITY_GROUP_ID" />
    <Key Column="APPLSYS.FND_APPLICATION.APPLICATION_ID" />
  </ObjectKey>
</ObjectNames>
<Tables>
  <Table Name="FND_USER_RESP_GROUPS_DIRECT" Schema="APPS" APK="" USN=""
WhereClause="" >
    <PK Column="SECURITY_GROUP_ID" />
    <PK Column="RESPONSIBILITY_ID" />
    <PK Column="RESPONSIBILITY_APPLICATION_ID" />
    <PK Column="USER_ID" />
  </Table>
  <Table Name="FND_APPLICATION" View="FND_APPLICATION#" Schema="APPLSYS"
APK="" USN="" WhereClause="" JoinParentTable="FND_USER_RESP_GROUPS_
DIRECT" JoinParentColumn="APPS.FND_USER_RESP_GROUPS_
DIRECT.RESPONSIBILITY_APPLICATION_ID" JoinChildColumn="APPLSYS.FND_
APPLICATION.APPLICATION_ID" >
```

```

        <PK Column="APPLSYS.FND_APPLICATION.APPLICATION_ID" />
</Table>
<Table Name="FND_USER" View="FND_USER#" Schema="APPLSYS" APK="USER_ID"
USN="LAST_UPDATE_DATE" WhereClause="" JoinParentTable="FND_USER_RESP_
GROUPS_DIRECT" JoinParentColumn="APPS.FND_USER_RESP_GROUPS_DIRECT.USER_
ID" JoinChildColumn="APPLSYS.FND_USER.USER_ID" >
        <PK Column="USER_NAME" />
</Table>
<Table Name="FND_SECURITY_GROUPS" View="FND_SECURITY_GROUPS#"
Schema="APPLSYS" APK="SECURITY_GROUP_ID" USN="LAST_UPDATE_DATE"
WhereClause="" JoinParentTable="FND_USER_RESP_GROUPS_DIRECT"
JoinParentColumn="APPS.FND_USER_RESP_GROUPS_DIRECT.SECURITY_GROUP_ID"
JoinChildColumn="APPLSYS.FND_SECURITY_GROUPS.SECURITY_GROUP_ID" >
        <PK Column="SECURITY_GROUP_ID" />
</Table>
<Table Name="FND_RESPONSIBILITY" View="FND_RESPONSIBILITY#"
Schema="APPLSYS" APK="" USN="" WhereClause="" JoinParentTable="FND_USER_
RESP_GROUPS_DIRECT" JoinParentColumn="APPS.FND_USER_RESP_GROUPS_
DIRECT.RESPONSIBILITY_ID, APPS.FND_USER_RESP_GROUPS_
DIRECT.RESPONSIBILITY_APPLICATION_ID" JoinChildColumn="APPLSYS.FND_
RESPONSIBILITY.RESPONSIBILITY_ID, APPLSYS.FND_
RESPONSIBILITY.APPLICATION_ID" >
        <PK Column="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID" />
        <ParentTableFK Column="APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID"
ParentColumn="APPLSYS.FND_APPLICATION.APPLICATION_ID" />
</Table>
</Tables>
<Functions>
    <Insert>
        <Function Name="$ebsUserPackageName$.AddResp">
            <Parameter Name="username" PropertyName="APPLSYS.FND_
USER.USER_NAME" PropertyType="CHAR" Mandatory="TRUE" />
            <Parameter Name="resp_app" PropertyName="APPLSYS.FND_
APPLICATION.APPLICATION_SHORT_NAME" PropertyType="CHAR"
Mandatory="TRUE" />
            <Parameter Name="resp_key" PropertyName="APPLSYS.FND_
RESPONSIBILITY.RESPONSIBILITY_KEY" PropertyType="CHAR"
Mandatory="TRUE" />
        </Function>
    </Insert>
</Functions>

```

```

    <Parameter Name="security_group" PropertyName="APPLSYS.FND_
    SECURITY_GROUPS.SECURITY_GROUP_KEY" PropertyType="CHAR"
    Mandatory="TRUE" />

    <Parameter Name="description" PropertyName="APPS.FND_USER_
    RESP_GROUPS_DIRECT.DESCRPTION" PropertyType="CHAR"
    Mandatory="TRUE" NullValue ="null" />

    <Parameter Name="start_date" PropertyName="APPS.FND_USER_
    RESP_GROUPS_DIRECT.START_DATE" PropertyType="DATE"
    Mandatory="TRUE" NullValue ="sysdate" />

    <Parameter Name="end_date" PropertyName="APPS.FND_USER_RESP_
    GROUPS_DIRECT.END_DATE" PropertyType="DATE" Mandatory="TRUE"
    NullValue ="null" />

</Function>
</Insert>
<Update>
    <Function Name="$ebsUserPackageName$.AddResp">
        <Parameter Name="username" PropertyName="APPLSYS.FND_
        USER.USER_NAME" PropertyType="CHAR" Mandatory="TRUE" />
        <Parameter Name="resp_app" PropertyName="APPLSYS.FND_
        APPLICATION.APPLICATION_SHORT_NAME" PropertyType="CHAR"
        Mandatory="TRUE" />
        <Parameter Name="resp_key" PropertyName="APPLSYS.FND_
        RESPONSIBILITY.RESPONSIBILITY_KEY" PropertyType="CHAR"
        Mandatory="TRUE" />
        <Parameter Name="security_group" PropertyName="APPLSYS.FND_
        SECURITY_GROUPS.SECURITY_GROUP_KEY" PropertyType="CHAR"
        Mandatory="TRUE" />
        <Parameter Name="description" PropertyName="APPS.FND_USER_
        RESP_GROUPS_DIRECT.DESCRPTION" PropertyType="CHAR"
        Mandatory="TRUE" NullValue ="null" />
        <Parameter Name="start_date" PropertyName="APPS.FND_USER_
        RESP_GROUPS_DIRECT.START_DATE" PropertyType="DATE"
        Mandatory="TRUE" NullValue ="sysdate" />
        <Parameter Name="end_date" PropertyName="APPS.FND_USER_RESP_
        GROUPS_DIRECT.END_DATE" PropertyType="DATE" Mandatory="TRUE"
        NullValue ="null" />

    </Function>
</Update>
<Delete>
    <Function Name="$ebsUserPackageName$.DelResp">

```

```
<Parameter Name="username" PropertyName="APPLSYS.FND_
USER.USER_NAME" PropertyType="CHAR" Mandatory="TRUE" />
<Parameter Name="resp_app" PropertyName="APPLSYS.FND_
APPLICATION.APPLICATION_SHORT_NAME" PropertyType="CHAR"
Mandatory="TRUE" />
<Parameter Name="resp_key" PropertyName="APPLSYS.FND_
RESPONSIBILITY.RESPONSIBILITY_KEY" PropertyType="CHAR"
Mandatory="TRUE" />
<Parameter Name="security_group" PropertyName="APPLSYS.FND_
SECURITY_GROUPS.SECURITY_GROUP_KEY" PropertyType="CHAR"
Mandatory="TRUE" />
</Function>
</Delete>
</Functions>
</Object>
</ObjectNames>
</EBSF12>
```

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](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

## A

- account definition 62
  - add to IT Shop 75
  - assign automatically 73
  - assign to all identities 73
  - assign to business role 73
  - assign to cost center 72
  - assign to customers 77
  - assign to department 72
  - assign to identities 71, 74
  - assign to location 72
  - assign to system roles 74
  - assign to user account 85
  - create 63
  - delete 78
  - IT operating data 68-69
  - manage level 65
- application role
  - target system managers 168
- APPS user 16
- attribute 149, 151
- authorization assignment
  - direct 109, 117-118
  - indirect 109
  - invalid 127

## B

- base object 33, 49

## C

- calculation schedule 52
  - deactivate 54
- category 132
- configuration parameter 11, 171
- connector schema
  - extend 39
- convert connection parameter 33
- customer 134, 154
  - account definition (initial) 77

## D

- data group 147
- data group unit 148
- default user accounts 89
- department 156
- direction of synchronization
  - direction target system 23, 31
  - in the Manager 23

## E

- email notification 107
- excluded attribute 151
- exclusion definition 122
- extended property
  - E-Business Suite permissions 145
  - user account 140

## G

group identity 90

## H

hierarchy filter 36  
HR person 134, 152

## I

identity 88  
    assign user account 85  
    delete 88  
identity assignment  
    manual 83  
    remove 83  
    search criteria 82  
    user account 86  
inheritance  
    category 125  
initialize system connection 38  
IT operating data  
    change 70  
IT Shop shelf  
    assign account definition 75  
    assign permissions 115

## J

Job server  
    edit 18, 163  
    load balancing 50  
    properties 164

## L

load balancing 50  
location 156  
log file 57  
login data 107

## M

menu 146  
    excluded 151

## N

NLog 57  
notification 107

## O

object  
    delete immediately 55  
    outstanding 55  
    publish 55  
offline mode 59  
outstanding object 55

## P

participant 134, 154  
password  
    initial 106-107  
password policy 95  
    assign 97  
    character sets 101  
    check password 106  
    conversion script 102, 104  
    default policy 97, 99

- display name 99
  - edit 98
  - error message 99
  - excluded list 105
  - failed logins 99
  - generate password 106
  - initial password 99
  - name components 99
  - password age 99
  - password cycle 99
  - password length 99
  - password strength 99
  - predefined 96
  - test script 102-103
  - permission
    - about IT Shop requests 143
    - add to IT Shop 115
    - assign business role 113
    - assign category 143
    - assign cost center 112
    - assign department 112
    - assign extended properties 145
    - assign location 112
    - assign responsibility 143
    - assign role 110
    - assign security group 143
    - assign system role 114
    - assign user account 110, 117
    - category 125
    - edit 143
    - edit assignment 117
    - effective 122
    - exclusion 122
    - inheriting through categories 132
    - inheriting through roles 110
    - inheriting through system roles 114
    - overview 145
    - overview of all assignments 128
    - remove assignment 117
    - risk index 143
    - validity period 120
  - personalized admin identity 90
  - process group 148
  - project template 178
  - provisioning
    - accelerate 50
- R**
- reset revision 57
  - reset start up data 57
  - responsibility 143, 151
    - validity 151
  - revision filter 37
  - risk assessment
    - permission 143
    - user account 134
- S**
- schema
    - changes 35
    - shrink 35
    - update 35
  - schema extension 39
  - schema type
    - add additionally 39
    - function definition 47
    - hierarchy 45
    - method definition 46
    - object definition 42

- object key definition 43
- parameter 48
- primary key 44
- table definition 43
- variable for language version 49
- scope 36
- security attribute 140, 149, 151
- security group 143, 149
- server function 167
- single object synchronization 49, 54
  - accelerate 50
- SQL statement 38
- start up configuration 33
- supplier 134, 153
- synchronization
  - accelerate 37
  - authorizations 15, 175
  - base object
    - create 32
  - calculation schedule 52
  - configure 23, 30
  - connection parameter 23, 30, 32
  - customize schema 30
  - different E-Business Suite systems 32
  - extended schema 32
  - HR data 27
  - identity data 27
  - only changes 37
  - participant 28
  - prerequisite 13
  - prevent 54
  - scope 30
  - simulate 57
  - start 23, 52
  - supplier 28
  - synchronization project
    - create 23
  - target system schema 32
  - user 15
  - variable 30
  - variable set 32
  - workflow 23, 31
- synchronization analysis report 57
- synchronization configuration
  - customize 30-32
- synchronization log 57
  - contents 29
  - create 29
  - display 53
- synchronization project
  - create 23
  - deactivate 54
  - edit 132
  - project template 178
- synchronization server 17
  - configure 17
  - edit 163
  - install 18
  - Job server 18
  - server function 167
  - system requirements 17
- synchronization user 16
- synchronization workflow
  - create 23, 31
- synchronize department 36
- synchronize single object 54
- system
  - account definition 130
  - application roles 10

- category 125
- edit 130
- identity assignment 82
- report 157
- specify category 132
- synchronization type 130
- target system manager 10, 168
- system connection
  - change 33
  - enabled variable set 35

## T

- target system
  - not available 59
- target system manager 168
  - specify 130
- target system synchronization 55
- template
  - IT operating data, modify 70

## U

- use case 146
- user access for Oracle E-Business Suite 16
- user account 133
  - administrative user account 90-92
  - apply template 70
  - assign extended properties 140
  - assign identity 80
  - assign permissions 118
  - assigned identity 134
  - assigned permissions 157
  - category 125
  - connected 85

- customer 134
- data quality 157
- deactivate 140, 142
- default user accounts 89
- delete 142
- delete identity 88
- edit authorization assignment 118
- group identity 90
- HR person 134
- identity 88, 92
- identity assignment 86
- login data 138
- manage level 84
- overview 140
- participant 134
- password 106, 138
  - notification 107
- personalized admin identity 90
- privileged user account 88, 93
- remove authorization assignment 118
- risk index 134
- security attribute 140
- set up 134
- status 134
- supplier 134
- type 88-90, 93
- unused 157

## V

- validity of permission assignments 120
- validity period 120
- variable set 33
  - active 35

## W

wrapper 16

## X

XOrigin 109, 127