



One Identity Manager 8.1

Administration Guide for Connecting to Oracle E-Business Suite

Copyright 2019 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Contents

Mapping an Oracle E-Business Suite in One Identity Manager	8
Architecture overview	8
One Identity Manager users for managing an Oracle E-Business Suite	9
Configuration parameters	10
Synchronizing an Oracle E-Business Suite	11
Setting up the initial synchronization	12
Users and permissions for synchronizing with Oracle E-Business Suite	13
How to prepare the synchronization user	14
Setting up the synchronization server	15
System requirements for the synchronization server	15
Installing the One Identity Manager Service	16
Creating a synchronization project for initial synchronization of Oracle E-Business Suite	18
Information required for setting up a synchronization project	19
Setting up an initial synchronization project	20
Setting up a synchronization project for employee data	23
Setting up a synchronization project for organizational data	24
Configuring the synchronization log	25
Customizing synchronization configuration	25
Important notes for adjusting existing synchronization projects	26
Configuring synchronization to the Oracle E-Business Suite	27
Configuring synchronization of several Oracle E-Business Suite systems	28
Updating schemas	29
Speeding up synchronization with revision filtering	30
Using specific statements for database initialization	30
Using additional schema types	31
Creating a schema extension file	33
Object definitions	34
Table definitions	35
Task definitions	38
Symbolic variables in WHERE clauses	41

Configuring single object synchronization	41
Executing a synchronization	42
Starting synchronizations	42
Displaying synchronization results	43
Deactivating synchronization	44
Synchronizing single objects	45
Tasks after a synchronization	45
Post-processing outstanding objects	45
Adding custom tables to the target system synchronization	47
Error analysis	48
Managing E-Business Suite user accounts and employees	49
Setting up account definitions	50
Creating account definitions	51
Master data for account definitions	51
Creating manage levels	53
Master data for manage levels	54
Creating mapping rules for IT operating data	55
Entering IT operating data	57
Modify IT operating data	59
Assigning account definitions to employees	60
Assigning account definitions to departments, cost centers, and locations	61
Assigning account definitions to business roles	61
Assigning account definitions to all employees	62
Assigning account definitions directly to employees	62
Assigning account definitions to system roles	63
Adding account definitions in the IT Shop	63
Assigning account definitions to target systems	65
Deleting account definitions	65
Automatic assignment of employees to E-Business Suite user accounts	67
Editing search criteria for automatic employee assignment	68
Finding employees and directly assigning them to user accounts	70
Changing the manage level in user accounts	71
Assigning account definitions to linked user accounts	72
Manually linking employees to E-Business Suite user accounts	72
Linking E-Business Suite user accounts to imported employees	73

Special features for the deletion of employees	75
Supported user account types	75
Default user accounts	77
Administrative user accounts	77
Privileged User Accounts	78
Assigning employees with specific permissions to a user account with shared identity	80
Provision of login information	81
Password policies for E-Business Suite user accounts	81
Predefined password policies	82
Applying password policies	83
Editing password policies	85
General master data for a password policy	85
Policy settings	86
Character classes for passwords	87
Custom scripts for password requirements	88
Script for checking a password	88
Script for generating a password	89
Editing the exclusion list for passwords	90
Checking passwords	90
Testing the generation of passwords	91
Initial password for new E-Business Suite user accounts	91
Email notifications about login data	92
Managing entitlement assignments	94
Assigning E-Business Suite entitlements to user accounts in One Identity Manager	95
Assigning E-Business Suite entitlements to departments, cost centers, and locations	96
Assigning E-Business Suite entitlements to business roles	97
E-Business Suite Include entitlements in system roles	98
E-Business Suite Adding entitlements to IT Shop	99
Assigning E-Business Suite user accounts directly to an entitlement	100
E-Business Suite Assigning entitlements directly to a user account	102
Validity period of permission assignments	104
Effectiveness of entitlement assignments	106
Inheritance of E-Business Suite entitlements based on categories	108
Invalid entitlement assignments	110

Overview of all assignments	111
Mapping of E-Business Suite objects in One Identity Manager	113
E-Business Suite systems	113
General master data for E-Business Suite systems	113
Defining categories for the inheritance of E-Business Suite entitlements	115
Editing a synchronization project	115
E-Business Suite User accounts	116
Entering master data for E-Business Suite user accounts	117
General master data for E-Business Suite user accounts	117
Login data for E-Business Suite user accounts	121
Additional tasks for managing E-Business Suite user accounts	121
Overview of E-Business Suite user accounts	122
Assigning extended properties to an E-Business Suite user account	122
E-Business Suite Disabling user accounts	123
Deleting E-Business Suite user accounts	124
E-Business Suite entitlements	124
Entering master data for E-Business Suite entitlements	125
General master data for E-Business Suite entitlements	125
Additional tasks for managing E-Business Suite entitlements	126
Overview of E-Business Suite entitlements	127
Assigning extended properties to an E-Business Suite entitlement	127
E-Business Suite applications	127
E-Business Suite Menus	128
E-Business Suite Data groups	129
E-Business Suite Data group units	129
E-Business Suite Request groups	130
E-Business Suite Security groups	130
E-Business Suite attributes	131
E-Business Suite responsibilities	131
Displaying master data for E-Business Suite responsibilities	132
General master data for E-Business Suite responsibilities	132
HR people	133
Suppliers and contacts	134
Parties	135
Locations	137

E-Business Suite object reports	137
Handling of E-Business Suite objects in Web Portal	139
Basic configuration data	141
Job server for E-Business Suite-specific process handling	142
Editing E-Business Suite Job servers	142
General master data for Job servers	143
Specifying server functions	145
Target system managers	146
Appendix: Access rights required for synchronization with an Oracle E-Business Suite	149
Appendix: Default project templates for synchronizing an Oracle E-Business Suite	151
Project template for user accounts and entitlements	151
Project templates for HR data	152
Project templates for CRM data	153
Project template for OIM data	153
Appendix: Editing system objects	154
Appendix: Configuration parameters for managing Oracle E-Business Suite	156
Appendix: Example of a schema extension file	160
About us	164
Contacting us	164
Technical support resources	164
Index	165

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.

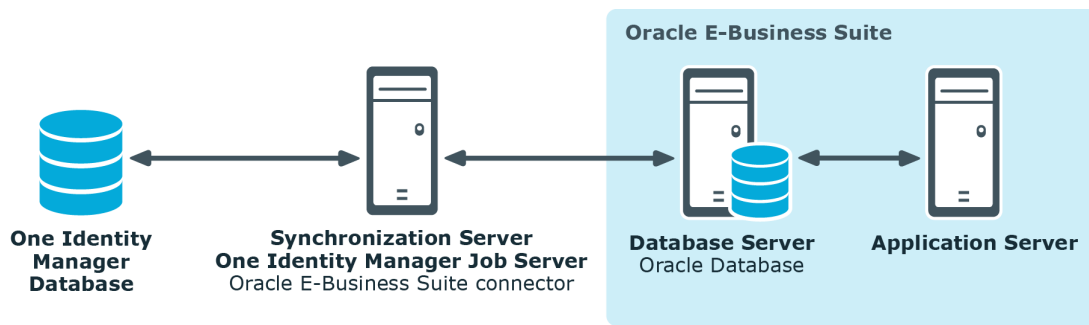
One Identity Manager provides company employees with the necessary user accounts. For this, you can use different mechanisms to connect employees to their user accounts. You can also manage user accounts independently of employees and therefore set up administrator user accounts.

In addition, data can be imported from the Human Resources module (employee 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 via 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 compared between the One Identity Manager database and Oracle Database.

Figure 1: Architecture for synchronization



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

The following users are used for setting up and managing an E-Business Suite system.

Table 1: Users

Users	Task
Target system administrators	<p>Target system administrators must be assigned to the Target systems Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Administrate application roles for individual target systems types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles are conflicting for target system managers • Authorize other employee to be target system administrators. • Do not assume any administrative tasks within the target system.
Target system managers	<p>Target system managers must be assigned to Target systems Oracle E-Business Suite or a sub-application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts or groups.

Users	Task
One Identity Manager administrators	<ul style="list-style-type: none"> • Edit password policies for the target system. • Prepare entitlements for adding to the IT Shop. • Can create employees with an identity that differs from the Primary identity. • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required. <hr/> <ul style="list-style-type: none"> • Create customized permissions groups for application roles for role-based login to administration tools in Designer as required. • Create system users and permissions groups for non-role-based login to administration tools in Designer as required. • Enable or disable additional configuration parameters in Designer as required. • Create custom processes in Designer as required. • Create and configures schedules as required. • Create and configure password policies as required.

Configuration parameters

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

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

For more information, see [Appendix: Configuration parameters for managing Oracle E-Business Suite](#) on page 156.

Synchronizing an Oracle E-Business Suite

The One Identity Manager supports synchronization with Oracle E-Business Suite 12.1 and 12.2. 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 an Oracle E-Business Suite to the One Identity Manager database,
- how to adjust a synchronization configuration, for example, to synchronize different E-Business Suite systems with the same synchronization project,
- how to start and deactivate the synchronization,
- how to evaluate the synchronization results.

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

Detailed information about this topic

- [Setting up the initial synchronization](#) on page 12
- [Customizing synchronization configuration](#) on page 25
- [Executing a synchronization](#) on page 42
- [Error analysis](#) on page 48
- [Appendix: Editing system objects](#) on page 154

Related Topics

- [Architecture overview](#) on page 8

Setting up the initial synchronization

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, the required processes are created that are used for the provisioning of 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 configuration parameter **TargetSystem | EBS** is set.
 - Check whether the configuration parameter is set in the Designer. Otherwise, set the configuration parameter and compile the database.
 - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
3. Install and configure a synchronization server and declare the server as 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 13
- [System requirements for the synchronization server](#) on page 15
- [Creating a synchronization project for initial synchronization of Oracle E-Business Suite](#) on page 18
- [Appendix: Configuration parameters for managing Oracle E-Business Suite](#) on page 156
- [Appendix: Default project templates for synchronizing an Oracle E-Business Suite](#) on page 151

Users and permissions for synchronizing with Oracle E-Business Suite

The following users are involved in synchronizing One Identity Manager with Oracle E-Business Suite.

Table 2: Users for synchronization

Users	Permissions
User for accessing the target system (synchronization user)	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 How to prepare the synchronization user on page 14 and Appendix: Access rights required for synchronization with an Oracle E-Business Suite on page 149.
One Identity Manager Service user account	<p>The user account for One Identity Manager Service requires rights to carry out operations at file level, for example, assigning user rights and creating and editing directories and files.</p> <p>The user account must belong to the Domain users group.</p> <p>The user account must have the Login as a service extended user right</p> <p>The user account requires access rights to the internal web service.</p> <p>NOTE: If One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access rights for the internal web service with the following command line call:</p> <pre>netsh http add urlacl url=http://<IP address>:<port number>/user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>The user account needs full access to the One Identity Manager installation directory in order to automatically update One Identity Manager Service.</p> <p>In the default installation the One Identity Manager is installed under:</p> <ul style="list-style-type: none"> • %ProgramFiles(x86)%\One Identity (on 32-bit operating systems) • %ProgramFiles%\One Identity (on 64-bit operating systems)
User for accessing the One Identity Manager database	The Synchronization default system user is provided for executing synchronization with 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.

The calling rights of standard packages have been changed in the Oracle E-Business Suite version 12.2 (from `CURRENT_USER AUTHID` to `DEFINER AUTHID`). To enable execution of 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 execute 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. The files are located on the One Identity Manager installation medium in the directory `.. | Modules | EBS | dvd | AddOn | SDK`.

To add the synchronization user

1. Add the wrapper package `FND_USER_Wrapper.sql` 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 variables `&&username` and `&&password`.

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

- [Appendix: Access rights required for synchronization with an Oracle E-Business Suite](#) on page 149

Setting up the synchronization server

All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.

The 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 15
- [Installing the One Identity Manager Service](#) on page 16

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
Following versions are supported:
 - Windows Server 2016
 - Windows Server 2012 R2
 - Windows Server 2012
 - Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later
- Microsoft .NET Framework Version 4.7.2 or later

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

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 known as a Job server in the 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 useful to set up a Job server for each target system on performance grounds. This avoids unnecessary swapping of connections to target systems because a Job server only has to process tasks of the same type (re-use of existing connections).

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

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

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

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

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

1. Start the program Server Installer on your administrative workstation.
2. Enter the valid connection credentials for the One Identity Manager database on the **Database connection** page.

3. Specify the server on which you want to install One Identity Manager Service on the **Server properties** page.
 - a. Select a Job server from the **Server** menu.
 - OR -
 - To create a new Job server, click **Add**.
 - b. Enter the following data for the Job server.

Table 4: Job Server Properties

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

4. Select **E-Business Suite** on the **Machine roles** page.
5. Select **Oracle E-Business Suite connector** on the **Server functions** page.
6. Check the One Identity Manager Service configuration on the **Service settings** page.

NOTE: The initial service configuration is predefined already. If further changes need to be made to the configuration, you can do this later with the Designer. For detailed information about configuring the service, see the *One Identity Manager Configuration Guide*.
7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. Select the directory with the install files on **Select installation source**.
10. Select the file with the private key on the page **Select private key file**.

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

Table 5: Installation Data

Data	Description
Computer	<p>Server on which to install and start the service from.</p> <p>To select a server</p> <ul style="list-style-type: none"> • Enter a name for the server. - OR - • Select a entry from the list.
Service account	<p>User account data for the One Identity Manager Service.</p> <p>To enter a user account for the One Identity Manager Service</p> <ul style="list-style-type: none"> • Set the option Local system account. This starts the One Identity Manager Service under the NT AUTHORITY\SYSTEM account. - OR - • Enter user account, password and password confirmation.
Installation account	<p>Data for the administrative user account to install the service.</p> <p>To enter an administrative user account for installation</p> <ul style="list-style-type: none"> • Enable Advanced. • Enable Current user. This uses the user account of the current user. - OR - • Enter user account, password and password confirmation.

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

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

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

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

Creating a synchronization project for initial synchronization of Oracle E-Business Suite

Use the Synchronization Editor to configure synchronization between the Oracle E-Business Suite database and One Identity Manager. The following describes the steps for initial configuration of a synchronization project for user accounts and permissions. For detailed

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 6: Information required for setting up a synchronization project

Data	Explanation
Server	Name of the server on which the Oracle Database is installed. The fully qualified server name or the IP address may be given.
Port and service name	Port of the Oracle instance and name of the service.
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 How to prepare the synchronization user on page 14.
Data source	TNS alias name from <code>TNSNames.ora</code> . This data is only required if the Oracle E-Business Suite connector can only access the Oracle Database through Oracle Clients.
Synchronization server for Oracle E-Business Suite	All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. For more information, see Setting up the synchronization server on page 15.
One Identity Manager database connection data	<ul style="list-style-type: none">• Database server• Database• SQL Server Login and password• Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.

Data	Explanation
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 target system to do this. Sometimes direct access from the workstation on which the Synchronization Editor is installed is not possible, because of the firewall configuration, for example, or because the workstation does not fulfill the necessary hardware and software requirements. If direct access to the workstation is not possible, you can set up a remote connection.</p> <p>The remote connection server and the workstation must be in the same Active Directory domain.</p> <p>Remote connection server configuration:</p> <ul style="list-style-type: none"> • One Identity Manager Service is started • RemoteConnectPlugin is installed • Oracle E-Business Suite connector is installed <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 you configure a synchronization project if Synchronization Editor is both:

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

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

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

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

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

2. Select **Target system type Oracle E-Business Suite** and click **Start**.

This starts the Synchronization Editor's project wizard.

3. Specify how One Identity Manager can access the target system on the **System access** page.
 - If access is possible from the workstation on which you started Synchronization Editor, you do not need to make any settings.
 - If access is not possible from the workstation on which you started Synchronization Editor, you can set up a remote connection.

Enable the **Connect using remote connection server** option and select the server to be used for the connection under **Job server**.
4. 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 7: Login information for connection to Oracle E-Business Suite

Property	Description
Direct access (without Oracle client)	Specifies whether the Oracle E-Business Suite connector has direct access to the Oracle Database database. Disable this option for access through Oracle clients. Which connection data is required, depends on how this option is set.
Server	Name of the server on which Oracle Database is installed. The fully qualified server name or the IP address may be given.
Port	Port of the Oracle instance.
Service name	Name of the service.
Users	User name used by the connector to log in to the Oracle Database.
Password	Password for logging in to the Oracle Database.
Data source	TNS alias name from TNSNames.ora.

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

5. Configure more default parameter for the connection on the **Further Connection Configuration** page.

Table 8: Connection Configuration

Property	Description
Language selection	Languages used to load captions from the database.
Unique name for	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

Property	Description
the DN.	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"> • User APPS (scenario 1): no input required. Default is APPS.FND_User_PKG. • Wrapper (scenario 2): name of the wrapper package. Default is APPS.FND_USER_WRAPPER. • Otherwise (scenario 3): name of the user package. Default is APPS.FND_User_PKG.

6. Enter a unique display name for the connection configuration on the **Display Name** page.

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.

7. You can save the connection data on the last page of the system connection wizard.
 - 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.
8. 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.

9. 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.
10. 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.

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

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

- a. Click  to add a new Job server.
- b. Enter a name for the Job server and the full server name conforming to DNS syntax.
- c. Click **OK**.

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

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

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

The synchronization project is created, saved and enabled immediately.

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

Related Topics

- [Configuring the synchronization log](#) on page 25
- [Customizing synchronization configuration](#) on page 25
- [Project template for user accounts and entitlements](#) on page 151
- [Setting up a synchronization project for employee data](#) on page 23
- [Setting up a synchronization project for organizational data](#) on page 24

Setting up a synchronization project for employee 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.

To set up a synchronization project for employee 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 20
- [Project templates for HR data](#) on page 152

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.

- i** **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.

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 person 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 20
- [Project templates for CRM data](#) on page 153
- [Project template for OIM data](#) on page 153

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.

To configure the content of the synchronization log

1. To configure the synchronization log for target system connection, select the category **Configuration | Target system** in Synchronization Editor.
- OR -
To configure the synchronization log for the database connection, select **Configuration | One Identity Manager connection** in Synchronization Editor.
2. Select the **General** view and click **Configure**.
3. Select the **Synchronization log** view and 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 analyses.

5. Click **OK**.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Related Topics

- [Displaying synchronization results](#) on page 43

Customizing synchronization configuration

Once you have set up a synchronization project for initial synchronization of an E-Business Suite host with the Synchronization Editor, 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 master 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 methods, for example.
- Use variables to set up a synchronization project which can be used for several 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 the database initialization, 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 detailed information about configuring synchronization, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- [Configuring synchronization to the Oracle E-Business Suite](#) on page 27
- [Configuring synchronization of several Oracle E-Business Suite systems](#) on page 28
- [Updating schemas](#) on page 29
- [Using specific statements for database initialization](#) on page 30
- [Using additional schema types](#) on page 31

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 employee data

If you change the mappings for synchronization of employee data for a specific company, check whether you also need to change which columns are locked in the Employee or Locality table. To lock additional columns for editing in One Identity Manager, define custom scripts (OnLoaded) in the Employee 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 changes via 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 detailed information about adjusting the connection parameters and editing variables, see *One Identity Manager Target System Synchronization Reference Guide*.

Configuring synchronization to the 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 master system during synchronization, you also require a workflow with synchronization in the direction of the **Target system**.

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

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

1. Open the synchronization project in the Synchronization Editor.
2. Check whether existing mappings can be used for synchronizing the target system. Create new maps if required.

3. Create a new workflow with the workflow wizard.
Creates a workflow with **Target system** as its synchronization direction.
4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Related Topics

- [Configuring synchronization of several Oracle E-Business Suite systems](#) on page 28

Configuring synchronization of several Oracle E-Business Suite systems

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

Prerequisites

- The target system schemas 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. Open the synchronization project in the Synchronization Editor.
3. Create a new base object for the other system. Use the wizards to attach a base object.
 - In the wizard, select the Oracle E-Business Suite connector and declare the connection parameters. The connection parameters are saved in a special variable set.
A start up configuration is created, which uses the newly created variable set.
4. Change other elements of the synchronization configuration as required.
5. Save the changes.
6. Run a consistency check.

Related Topics

- [Configuring synchronization to the Oracle E-Business Suite](#) on page 27

Updating schemas

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

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

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

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

To update a system connection schema

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Configuration | Target systems**.
- OR -
Select the category **Configuration | One Identity Manager connection**.
3. Select the view **General** and click **Update schema**.
4. Confirm the security prompt with **Yes**.
This reloads the schema data.

To edit a mapping

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

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

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 its last execution date as a revision in the the One Identity Manager database (table `DPRRevisionStore`, column `Value`). This value is used as a comparison for revision filtering when the same workflow is synchronized the next time. When this workflow is synchronized the next time, the 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.

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

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

To permit revision filtering on a workflow

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

To permit revision filtering for a start up configuration

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

For detailed 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 executed every time a connection is established.

To use additional statements for database initialization:

1. Open the synchronization project in the Synchronization Editor.
2. Enable expert mode.
3. Edit the target system connection.
 - a. Select the category **Configuration | Target systems**.
 - b. Click **Edit connection**.

This starts the system connection wizard.
 - c. Select **Database connection startup sequence** and enter the SQL statements to be executed every time a connection is established.
 - 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 category **Configuration | Target systems**.
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 33.
3. Open the synchronization project in the Synchronization Editor.
4. Enable expert mode.
5. Select the category **Configuration | Target systems**.
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 category **Mapping** and create mappings for the your new schema types. Take note of whether these are read-only or whether read/write access is permitted.
For detailed information about setting up mapping and schema classes, see the *One Identity Manager Target System Synchronization Reference Guide*.
14. Select the **Workflows** category and edit the workflows. Create additional synchronization steps for the new mappings. Take note of whether the schema types are read-only or whether read/write access is permitted.
For detailed information about creating 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 delete the schema from the schema extension file:

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 contain 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 34
- [Table definitions](#) on page 35

- [Task definitions on page 38](#)
- [Appendix: Example of a schema extension file on page 160](#)

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 9: 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 false .
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 true .
UseDistinct	Specifies whether duplicate entries are prevented through the use of the Distinct function. The default value is false .

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 10: 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 false .
IsDNColumn	Specifies whether the value in this column is inserted as a component into the defined name of the object. The default value is false .
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 11: 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 LAST_UPDATE_DATE 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.
JoinParentColumn	Comma-delimited list of columns in a superordinate table, if a Join operation is to be executed for a hierarchically superordinate schema type (full notation).
JoinChildColumn	Comma-delimited list of columns in the currently defined table that shall be joined to the columns from JoinParentColumn in the Join operation (full notation). The sequence of columns in the list determines which columns are joined to each other.

Example

<Tables>

```
<Table Name="FND_RESPONSIBILITY_TL" Schema="APPLSYS" APK="" USN=""
WhereClause="APPLSYS.FND_RESPONSIBILITY_TL.LANGUAGE='US'"
JoinParentColumn="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID,APPLSYS.FND_
RESPONSIBILITY.APPLICATION_ID" 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 12: Attribute of a primary key definition

Attribute	Description
Column	Name of the primary key column.

Example

```
<PK Column="REQUEST_GROUP_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 13: 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"
      IsDNCColumn="true" IsReferencedColumn="true" X500Abbreviation="RE" />
    <Key Column="APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID" />
  </ObjectKey>
  <Tables>
    <Table Name="FND_RESPONSIBILITY" Schema="APPLSYS" APK="" USN=""
      WhereClause="" JoinParentColumn="" JoinChildColumn="" >
      <PK Column="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID" />
      <ParentTableFK Column="APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID"
        ParentColumn="APPLSYS.FND_APPLICATION.APPLICATION_ID" />
    </Table>
    <Table Name="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" JoinChildColumn="APPLSYS.FND_RESPONSIBILITY_
        TL.RESPONSIBILITY_ID,APPLSYS.FND_RESPONSIBILITY_TL.APPLICATION_ID" >
      <PK Column="APPLSYS.FND_RESPONSIBILITY_TL.RESPONSIBILITY_ID" />
    </Table>
    <Table Name="FND_APPLICATION" Schema="APPLSYS" APK="" USN="" WhereClause=""
```

```

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 (IsDNColumn="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 41.

Task definitions

The <Functions> tag enables you to define methods within the object definition that can be executed for objects of the schema type. Each method executes 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 executed 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 executed that are placed in a fixed order based on their OrderNumber attribute. When the Delete method is called, only one defined function is executed.

Function definitions

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

Table 14: 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 execution sequence. The default value is 1 .

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 executing 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 execution of 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 20.

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 15: 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">• CHAR: Character string.• DATE: Date value. This value is converted as a valid date.• FIX: Fixed string value. The fixed value specified in the PropertyName attribute is always transferred.• NUM: Numerical value. The conversion does not permit any alpha-numeric characters.
Mandatory	Specifies whether the parameter is mandatory. The default value is false .
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 null is transferred. In this case, an optional parameter is not transferred to the function call. There are three cases in which a null value definition is practical: <ol style="list-style-type: none">a. Use of a constant defined in the function package, for example \$ebsUserPackageName\$.null_number. In this case, the name of the function package stored in the connection configuration is used for user account modification, if the variable expression \$ebsUserPackageName\$ is detected.b. Use of a symbolic constant defined in Oracle Database, for example sysdate.c. Use of a specific expression not equal to null, for example to_date('-2', 'J').

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 execution of the SQL statement.

Example

```
<Table Name="FND_SECURITY_GROUPS_TL" Schema="APPLSYS" APK="" USN=""  
WhereClause="APPLSYS.FND_SECURITY_GROUPS_TL.LANGUAGE='$$SYSLANGU$' "  
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 a member list belongs to one of these properties, then the entries in the allocation table will also be updated. 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 detailed information, see *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 **Oracle E-Business Suite | Basic configuration data | Target system types**.
2. In the result list, select the target system type **Oracle E-Business Suite**.
3. Select **Assign synchronization tables**.
4. In **Add assignments**, assign the custom table for which you want to use single object synchronization.
5. Save the changes.
6. Select **Configure tables for publishing**.
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 45
- [Post-processing outstanding objects](#) on page 45

Executing a 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 was terminated unexpectedly, you must reset the start information to be able to restart synchronization.

Detailed information about this topic

- [Starting synchronizations](#) on page 42
- [Deactivating synchronization](#) on page 44
- [Displaying synchronization results](#) on page 43

Starting synchronizations

When setting up the initial synchronization project using the Launchpad, a default schedule for regular synchronizations is created and assigned. To execute regular synchronizations, activate this schedule.

To synchronize on a regular basis

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

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

To start initial synchronization manually


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

- !** **IMPORTANT:** As long as synchronization is running, you must not start another synchronization for the same target system. This applies especially, if the same synchronization objects would be processed.
- If another synchronization is started with the same start up configuration, this process is stop and is assigned the **Frozen** execution status. An error message is written to the One Identity Manager Service log file.
 - If another synchronization is started with another start up configuration, that addresses same target system, it may lead to synchronization error or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration. 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. Open the synchronization project in the Synchronization Editor.
2. Select **Logs**.
3. Click  in the navigation view toolbar.

Logs for all completed synchronization runs are displayed in the navigation view.

4. Select a log by double-clicking on it.

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

To display a provisioning log.

1. Open the synchronization project in the Synchronization Editor.
2. Select **Logs**.
3. Click  in the navigation view toolbar.
Logs for all completed provisioning processes are displayed in the navigation view.
4. Select a log by double-clicking on it.

An analysis of the provisioning is show as a report. You can save the report.

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

Related Topics

- [Configuring the synchronization log](#) on page 25
- [Error analysis](#) on page 48

Deactivating synchronization

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

To prevent regular synchronization

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

Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

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

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. If a member list belongs to one of these properties, then the entries in the allocation table will also be updated.

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 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 **Synchronize this object**.

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

Detailed information about this topic

- [Configuring single object synchronization](#) on page 41

Tasks after a synchronization

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

- [Post-processing outstanding objects](#) on page 45

Post-processing outstanding objects

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

Outstanding objects

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

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

Start target system synchronization to do this.

To post-process outstanding objects

1. In the manager, select the **Oracle E-Business Suite | Target system synchronization: Oracle E-Business Suite** category.

All tables assigned to the target system type **Oracle E-Business Suite** as synchronization tables are displayed in the navigation view.

2. On the **Target system synchronization** form, in the **Table / object** column, open the node of the table for which you want to post-process outstanding objects.

All objects that are marked as outstanding are shown. The **Last log entry** and **Last method run** columns display the time at which the last entry was made in the synchronization log and which processing method was executed. The **No log available** entry can mean the following:

- The synchronization log has already been deleted.
- OR -
- An assignment from a member list has been deleted in the target system.
The base object of the assignment has been updated during the synchronization. A corresponding entry appears in the synchronization log. The entry in the assignment table is marked as outstanding, but there is no entry in the synchronization log.
- An object that contains a member list has been deleted in the target system.
During synchronization, the object and all corresponding entries in assignment tables are marked as outstanding. However, an entry in the synchronization log appears only for the deleted object.



TIP:


To display object properties of an outstanding object

- a. Select the object on the target system synchronization form.
- b. Open the context menu and click **Show object**.

3. Select the objects you want to rework. Multi-select is possible.
4. Click one of the following icons in the form toolbar to execute the respective method.

Table 16: Methods for handling outstanding objects

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

Icon	Method	Description
		is removed for the object.
		The method triggers the <code>HandleOutstanding</code> event. This runs a target system specific process that triggers the provisioning process for the object.
		Prerequisites: <ul style="list-style-type: none"> • The table containing the object can be published. • The target system connector has write access to the target system.
	Reset	The Outstanding label is removed for the object.

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

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

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

To disable bulk processing

- Deactivate  in the form 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. This means that the **Connection is read only** option is not set in the target system connection.

Adding custom tables to the target system synchronization

You must customize synchronization to synchronize custom tables.

To add tables to the target system synchronization

1. In the result list, select the target system type **Oracle E-Business Suite**.
2. Select **Assign synchronization tables**.
3. Assign custom tables whose outstanding objects you want to handle in **Add assignments**.
4. Save the changes.
5. Select **Configure tables for publishing**.

6. Select custom tables whose outstanding objects can be published in the target system and set **Publishable**.
7. Save the changes.

Related Topics

- [Post-processing outstanding objects](#) on page 45

Error analysis

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**
The 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 was terminated 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 the objects is now older than before the last synchronization. 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 43

Managing E-Business Suite user accounts and employees

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

Because requirements vary between companies, One Identity Manager offers different methods for supplying user accounts to employees. One Identity Manager supports the following method for linking employees and their user accounts.

- Employees can automatically obtain their account definitions using user account resources. If an employee does not yet have a user account in an E-Business Suite system, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism and subsequent process handling.

When you manage account definitions through user accounts, you can specify the way user accounts behave when employees are enabled or deleted.

- When user accounts are inserted, they can be automatically assigned to an existing employee. This mechanism can be implemented if a new user account is created manually or by synchronization. However, this procedure is not the default procedure for One Identity Manager. Define criteria for finding employees for automatic employee assignment.
- Employees and user accounts can be entered manually and assigned to each other.

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

- can be assigned to E-Business Suite user accounts as HR persons.
- can be linked to user accounts via automatic employee assignment, account definitions, or manually.

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

Related Topics

- [Setting up account definitions](#) on page 50
- [Automatic assignment of employees to E-Business Suite user accounts](#) on page 67
- [Entering master data for E-Business Suite user accounts](#) on page 117
- [Linking E-Business Suite user accounts to imported employees](#) on page 73

Setting up account definitions

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

The data for the user accounts in the respective target system comes from the basic employee data. The employees must have a E-Business Suite user account. The assignment of the IT operating data to the employee's user account is controlled through the primary assignment of the employee to a location, a department, a cost center, or a business role (template processing). Processing is done through templates. There are predefined templates for determining the data required for user accounts included in the default installation. You can customize templates as required.


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

The following steps are necessary to implement an account definition:

- [Creating account definitions](#)
- [Creating manage levels](#)
- [Creating mapping rules for IT operating data](#)
- [Entering IT operating data](#)
- [Assigning account definitions to employees](#)
- (Optional) [Assigning account definitions to target systems](#)

Creating account definitions

To create a new account definition

1. In the Manager, select **Oracle E-Business Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list. Select **Change master data**.
- OR -
Click  in the result list toolbar.
3. Enter the account definition's master data.
4. Save the changes.

Master data for account definitions

Enter the following data for an account definition:

Table 17: Master 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	Required account definitions. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is automatically requested or assigned with it. Leave empty for E-Business Suite systems.
Description	Spare text box 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 account definition assignments to employees. Enter a value between 0 and 1. This input field is only visible if the configuration parameter QER CalculateRiskIndex is activated. For more detailed information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .

Property	Description
Service item	Service item through which you can request the account definition in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. The account definition can also be assigned directly to employees and roles outside of IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	<p>Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added.</p> <p>i IMPORTANT: Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system.</p> <p>Disable this option to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees 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 disabled employees.</p> <p>Option set: The account definition assignment remains in effect. The user account stays the same.</p> <p>Option not set: 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 disabled employees.</p> <p>Option set: The account definition assignment remains in effect. The user account stays the same.</p> <p>Option not set: The account definition assignment is not in effect. The associated user account is disabled.</p>
Retain account definition on deferred	<p>Specifies the account definition assignment on deferred deletion of employees.</p> <p>Option set: The account definition assignment remains in effect. The user account stays the same.</p>

Property	Description
deletion	Option not set: 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 employees posing a security risk.</p> <p>Option set: The account definition assignment remains in effect. The user account stays the same.</p> <p>Option not set: 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 Designer to customize display names, formats and templates for the input fields.

Creating manage levels

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

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

One Identity Manager supplies a default configuration for manage levels:

- **Unmanaged:** User accounts with the **Unmanaged** manage level are linked to the employee but they do not inherit any further properties. When a new user account is added with this manage level and an employee is assigned, some of the employee's properties are transferred initially. If the employee properties are changed at a later date, the changes are not passed onto the user account.
- **Full managed:** User accounts with the **Full managed** manage level inherit defined properties of the assigned employee. When a new user account is created with this manage level and an employee is assigned, the employee's properties are transferred in an initial state. If the employee properties are changed at a later date, the changes are passed onto the user account.

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

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

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


- Employee user accounts can be locked when they are disabled, deleted or rated as a security risk so that permissions are immediately withdrawn. If the employee is 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 employee's user accounts are disabled and therefore cannot be members in groups. During this time, no inheritance processes should be calculated for this employee. Existing group memberships are deleted!

To assign manage levels to an account definition

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

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

To edit a manage level

1. Select **Oracle E-Business Suite | Basic configuration data | Account definitions | Manage levels**.
2. Select the manage level in the result list. Select **Change master data**.
- OR -
Click  in the result list toolbar.
3. Edit the manage level's master data.
4. Save the changes.

Master data for manage levels

Enter the following data for a manage level.

Table 18: Master Data for a Manage Level

Property	Description
Manage level	Name of the manage level.
Description	Spare text box 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"> • Never: Data is not updated. • Always: Data is always updated. • Only initially: The data is only determined at the start.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily disabled employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently disabled employees retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently disabled employees are locked.
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion retain their group memberships.
Lock user accounts if deletion is deferred	Specifies whether user accounts of employees marked for deletion are locked.
Retain groups on security risk	Specifies whether user accounts of employees posing a security risk retain their group memberships.
Lock user accounts if security is at risk	Specifies whether user accounts of employees posing a security risk are locked.
Retain groups if user account disabled	Specifies whether locked user accounts retain their group memberships.

Related Topics

- [Invalid entitlement assignments](#) on page 110

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 employee's primary roles.

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

- Groups can be inherited
- Identity
- Privileged user account

To create a mapping rule for IT operating data

1. In the Manager, select **Oracle E-Business Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.

3. Select **Edit IT operating data mapping** and enter the following data.

Table 19: Mapping rule for IT operating data

Property	Description
Column	User account property for which the value is set. In the menu, you can select the columns that use the <code>TSB_ITDataFromOrg</code> script in their template. For detailed information, see <i>One Identity Manager Target System Base Module Administration Guide</i> .
Source	<p>Specifies which roles to use in order to find the user account properties. You have the following options:</p> <ul style="list-style-type: none"> • Primary department • Primary location • Primary cost center • Primary business roles <p>i NOTE: Only use the primary business role if the Business Roles Module is installed.</p> <ul style="list-style-type: none"> • Empty <p>If you select a role, you must specify a default value and set the option Always use default value.</p>
Default value	Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.
Always use default value	Specifies whether user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.
Notify when applying the standard	Specifies whether email notification to a defined mailbox is sent when the default value is used. The Employee - new user account with default properties created mail template is used. To change the mail template, adjust the TargetSystem EBS Accounts MailTemplateDefaultValues configuration parameter.

4. Save the changes.

Entering IT operating data

To create user accounts with the **Full managed** manage level, the required IT operating data must be determined. The operating data required to automatically supply an employee with IT resources is shown in the departments, locations, cost centers, and business roles. An employee is assigned to one primary location, one primary department, one primary cost center or one primary business role. The necessary IT operating data is

ascertained from these assignments and used in creating the user accounts. Default values are used if valid IT operating data cannot be found over the primary roles.

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

Example

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


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

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

To define IT operating data

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

Table 20: IT operating data

Property	Description
Organization/Business role	Department, cost center, location or business role for which the IT operating data is valid.
Effects on	IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.
	<p>To specify an application scope</p> <ol style="list-style-type: none"> a. Click  next to the text box. b. Under Table, select the table that maps the target system for select the TSBAccountDef table for an account definition. c. Select the specific target system or account definition under Effects on. d. Click OK.
Column	User account property for which the value is set.

Property	Description
	In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For detailed information, see <i>One Identity Manager Target System Base Module Administration Guide</i> .
Value	Concrete value which is assigned to the user account property.

3. Save the changes.

Modify IT operating data

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

Prerequisites

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

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

To execute the template

1. In the Manager, select **Oracle E-Business Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Execute templates** in the task view

This displays a list of all user account, which are created through the selected account definition and whose properties are changed by modifying the IT operating data.

Old Current value of the object property.

value:

New Value that the object property would have following modification of the value:
IT operating data.

Selection: Specifies whether the modification shall be adopted for the user account.

4. Mark all the object properties in the **selection** column that will be given the new value.
5. Click **Apply**.

The templates are applied to all selected user accounts and properties.

Assigning account definitions to employees

Account definitions are assigned to company employees.

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

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

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

- ① **NOTE:** If a user account already exists and is disabled, then it is re-enabled. You have to alter the user account manage level afterwards in this case.

Prerequisites for indirect assignment of account definitions to employees

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

- ① **NOTE:** As long as an account definition for an employee is valid, the employee retains the user account that was created by it. If the assignment of an account definition is removed, the user account that was created from this account definition is disabled.

For detailed 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

To add account definitions to hierarchical roles

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

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

To remove an assignment

- Select the organization and double click .

5. Save the changes.

Assigning account definitions to business roles

Installed modules: Business Roles Module

To add account definitions to hierarchical roles

1. In the Manager, select **Oracle E-Business Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign business roles**.
4. Assign business roles in **Add assignments**.

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

To remove an assignment

- Select the business role and double click .

5. Save the changes.

Assigning account definitions to all employees

To assign an account definition to all employees

1. In the Manager, select **Oracle E-Business Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Change master data**.
4. Set **Automatic assignment to employees on General**.

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

5. Save the changes.

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

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

Assigning account definitions directly to employees

To assign an account definition directly to employees

1. In the Manager, select **Oracle E-Business Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign to employees**.
4. Assign employees in **Add assignments**.

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

To remove an assignment

- Select the employee and double click .

5. Save the changes.

Assigning account definitions to system roles

Installed modules: System Roles Module


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

To add account definitions to a system role

1. In the Manager, select **Oracle E-Business Suite | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign system roles**.
4. Assign system roles in **Add assignments**.

- 1 **TIP:** In the **Remove assignments** area, you can remove the assignment of system roles.

To remove an assignment

- Select the system role and double click .

5. Save the changes.

Adding account definitions in the IT Shop

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

- The account definition must be labeled with the **IT Shop** option.
- The account definition must be assigned to a service item.
 - 1 **TIP:** In Web Portal, all products that can be requested are grouped together by service category. To make the account definition easier to find in Web Portal, assign a service category to the service item.
- If the account definition is only assigned to employees using IT Shop assignments, you must also set **Only for use in IT Shop**. Direct assignment to hierarchical roles may not be possible.

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

To add an account definition to the IT Shop

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

To remove an account definition from individual IT Shop shelves

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

To remove an account definition from all IT Shop shelves

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

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

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

Related Topics

- [Master data for account definitions](#) on page 51

Assigning account definitions to target systems

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

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

User accounts are only linked to the employee (**Linked**) if no account definition is given.

To assign the account definition to a target system

1. In Manager, select the system in **Oracle E-Business Suite | Systems**.
2. Select **Change master data**.
3. Select the account definition for user accounts from **Account definition (initial)**.
4. Save the changes.

Detailed information about this topic

- [Automatic assignment of employees to E-Business Suite user accounts](#) on page 67

Deleting account definitions

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

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
 - a. In the Manager, select **Oracle E-Business Suite | Basic configuration data | Account definitions | Account definitions**.
 - b. Select an account definition in the result list.
 - c. Select **Change master data**.
 - d. Disable **Automatic assignment to employees** on the **General** tab.
 - e. Save the changes.
2. Remove direct assignments of the account definition to employees.
 - a. In the Manager, select **Oracle E-Business Suite | Basic configuration data | Account definitions | Account definitions**.
 - b. Select an account definition in the result list.


- c. Select **Assign to employees**.
 - d. Remove employees from **Remove assignments**.
 - e. Save the changes.
3. Remove the account definition's assignments to departments, cost centers and locations.
 - a. In the Manager, select **Oracle E-Business Suite | Basic configuration data | Account definitions | Account definitions**.
 - b. Select an account definition in the result list.
 - c. Select **Assign organizations**.
 - d. In **Remove assignments**, remove the relevant departments, cost centers, and locations.
 - e. Save the changes.
 4. Remove the account definition's assignments to business roles.
 - a. In the Manager, select **Oracle E-Business Suite | Basic configuration data | Account definitions | Account definitions**.
 - b. Select an account definition in the result list.
 - c. Select **Assign business roles**.
Remove the business roles in **Remove assignments**.
 - d. Save the changes.
 5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.

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

To remove an account definition from all IT Shop shelves

- a. In the Manager, select **Oracle E-Business Suite | Basic configuration data | Account definitions | Account definitions** (with non-role-based login).
- OR -
In the Manager, select **Entitlements | Account definitions** (with role-based login).
- b. Select an account definition in the result list.
- c. Select **Remove from all shelves (IT Shop)**.
- d. Confirm the security prompt with **Yes**.
- e. Click **OK**.


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

6. Remove the account definition assignment as required account definition for another account definition. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.
 - a. In the Manager, select **Oracle E-Business Suite | Basic configuration data | Account definitions | Account definitions**.
 - b. Select an account definition in the result list.
 - c. Select **Change master data**.
 - d. Remove the account definition in the **Required account definition** menu.
 - e. Save the changes.
7. Remove the account definition's assignments to target systems.
 - a. In Manager, select the system in **Oracle E-Business Suite | Systems**.
 - b. Select **Change master data**.
 - c. Remove the assigned account definitions on the **General** tab.
 - d. Save the changes.
8. Delete the account definition.
 - a. In the Manager, select **Oracle E-Business Suite | Basic configuration data | Account definitions | Account definitions**.
 - b. Select an account definition in the result list.
 - c. Click  to delete an account definition.

Automatic assignment of employees to E-Business Suite user accounts

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

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

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

Run the following tasks to assign employees automatically.

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

Example:

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

- Use the configuration parameter **TargetSystem | EBS | PersonAutoDisabledAccounts** to specify whether employees can be automatically assigned to disabled user accounts. User accounts do not obtain an account definition.
- Assign an account definition to the E-Business Suite system. Ensure that the manage level to be used is entered as the default manage level.
- Define the search criteria for employee assignment to this system.

i NOTE:

The following applies for synchronization:

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

The following applies outside synchronization:

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

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

Related Topics

- [Creating account definitions](#) on page 51
- [Assigning account definitions to target systems](#) on page 65
- [Changing the manage level in user accounts](#) on page 71
- [Editing search criteria for automatic employee assignment](#) on page 68

Editing search criteria for automatic employee assignment

The criteria for employee assignment are defined for the E-Business Suite system. In this case, you specify which user account properties must match the employee's properties such that the employee can be assigned to the user account. You can limit search criteria

further by using format definitions. The search criterion is written in XML notation to the **Search criteria for automatic employee assignment** column (AccountToPersonMatchingRule) in the EBSSystem table.

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

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

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

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

To specify criteria for employee assignment

1. Select the category **Oracle E-Business Suite | Systems**.
2. Select the E-Business Suite system in the result list.
3. Select **Define search criteria for employee assignment** in the task view.
4. Specify which user account properties must match with which employee so that the employee is linked to the user account.

Table 21: Standard search criteria for user accounts

Apply to	Column for employee	Column for user account
E-Business Suite User accounts	E-Business Suite User account (CentralEBSAccount)	User name (UserName)
	Person (UID_Person)	HR person (UID_PersonEmployee)

5. Save the changes.

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

Related Topics

- [Automatic assignment of employees to E-Business Suite user accounts](#) on page 67
- [Finding employees and directly assigning them to user accounts](#) on page 70

Finding employees and directly assigning them to user accounts

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

Table 22: Manual Assignment View

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

To apply search criteria to user accounts

1. Select **Oracle E-Business Suite | Systems** in the manager.
2. In the result list, select the E-Business Suite system.
3. Select **Define search criteria for employee assignment** in the task view.
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 employee master data.

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

To assign employees directly over a suggestion list

- Click **Suggested assignments**.
 1. Click **Selection** for all user accounts to which you want to assign the suggested employees. Multi-select is possible.
 2. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level**

menu.

3. Click **Assign selected**.
4. Confirm the security prompt with **Yes**.

The employees 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 employee assignment**.
 1. Click **Select employee** for the user account to which you want to assign an employee. Select an employee from the menu.
 2. Click **Selection** for all user accounts to which you want to assign the selected employees. Multi-select is possible.
 3. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level** menu.
 4. Click **Assign selected**.
 5. Confirm the security prompt with **Yes**.

The employees displayed in the **Employee** 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 **Selection** for all user accounts for which you want to delete the employee assignment. Multi-select is possible.
 2. Click **Remove selected**.
 3. Confirm the security prompt with **Yes**.

The assigned employees 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 employee assignment. You can change a user account manage level later.

To change the manage level for a user account

1. In Manager, select **Oracle E-Business Suite | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data**.

4. On the **General** tab, select the manage level in the **Manage level** menu.
5. Save the changes.

Related Topics

- [General master data for E-Business Suite user accounts](#) on page 117

Assigning account definitions to linked user accounts

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

- employees and user accounts have been linked manually
- automatic employee assignment is configured, but an account definition is not yet 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 the user accounts in a "linked" state.
 - a. Select **Oracle E-Business Suite | User accounts | Linked but not configured | <System>**.
 - b. Select **Assign account definition to linked accounts**.

Detailed information about this topic

- [Assigning account definitions to target systems](#) on page 65

Manually linking employees to E-Business Suite user accounts

An employee 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 employee can also use default user accounts with different types.

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

To manually assign user accounts to an employee

1. Select the **Employees | Employees**.
2. Select the employee in the result list and run **Assign E-Business Suite user accounts** from the task view.
3. Assign the user accounts.
4. Save the changes.

Related Topics

- [Supported user account types](#) on page 75

Linking E-Business Suite user accounts to imported employees

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

To assign an imported employee to a user account

1. Select the category **Oracle E-Business Suite | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data**.
4. Select the **General** tab.
5. Select the HR person from the **HR person** menu.
 - OR -
 - Select the customer from the **Customer** menu.
 - OR -
 - Select the supplier from the **Supplier** menu.
6. Save the changes.

If the imported employees are only connected to the user accounts through these columns, the user accounts are not managed by One Identity Manager. If an employee 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 employees for the imported employees, you can create connected user accounts. In these account, persons are connected to the user accounts via the column EBSUser.UID_Person.

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

Table 23: Persons assigned to user accounts

Property	Description
Person (UID_ Person)	Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. If you are using automatic employee assignment, an associated employee is found and added to the user account when you save the user account. Every active person can be assigned.
Customer (UID_ PersonCustomer)	Reference to an employee who is managed as a customer. Only employees from the E-Business Suite AR data source can be assigned (Person.ImportSource='EBSOIM').
HR person (UID_ PersonEmployee)	Reference to an employee in the Human Resources module of Oracle E-Business Suite. Only employees from the E-Business Suite HR data source can be assigned (Person.ImportSource='EBSHR').
Party (UID_ PersonParty)	Reference to an employee who is managed as a party. An employee with the E-Business Suite AR data source can be assigned (Person.ImportSource='EBSOIM'). The assignment cannot be edited in One Identity Manager.
Supplier (UID_ PersonSupplier)	Reference to an employee who is managed as a supplier or a contact. Only employees from the E-Business Suite AP data source can be assigned (Person.ImportSource='EBSCRIM').

Detailed information about this topic

- [Managing E-Business Suite user accounts and employees](#) on page 49
- [Editing search criteria for automatic employee assignment](#) on page 68

Related Topics

- [Setting up a synchronization project for employee data](#) on page 23
- [Setting up a synchronization project for organizational data](#) on page 24
- [HR people](#) on page 133
- [Parties](#) on page 135
- [Suppliers and contacts](#) on page 134

Special features for the deletion of employees

If an employee 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 employee after the deferred deletion has expired. If the user account is managed using an account definition, the behavior on deletion of the connected person is defined in the account definition. User accounts cannot be deleted in One Identity Manager. The person 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 status **INACTIVE**.

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

Related Topics

- [Deleting E-Business Suite user accounts](#) on page 124
- [E-Business Suite Disabling user accounts](#) on page 123

Supported user account types

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

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

- Identity

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

Table 24: Identities of user accounts

Identity	Description	Value of the IdentityType column
Primary identity	Employee's default user account.	Primary
Organizational identity	Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.	Organizational

Identity	Description	Value of the IdentityType column
Personalized admin identity	User account with administrative permissions, used by one employee.	Admin
Sponsored identity	User account that is used for training purposes, for example.	Sponsored
Shared identity	User account with administrative permissions, used by several employees.	Shared
Service identity	Service account.	Service

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

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

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

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

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

- Privileged user account

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

Detailed information about this topic

- [Default user accounts](#) on page 77
- [Administrative user accounts](#) on page 77
- [Privileged User Accounts](#) on page 78

Default user accounts

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

To create default user accounts through account definitions

1. Create an account definition and assign the **Unmanaged** and **Full managed** manage levels.
2. Specify the effect of temporarily or permanently disabling, deleting or the security risk of an employee on its user accounts and group memberships for each manage level.
3. Create a formatting rule for IT operating data.

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

Which IT operating data is required depends on the target system. The following settings are recommended for default user accounts:

- In the mapping rule for the `IsGroupAccount` column, use the default value **1** and enable **Always use default value**.
 - In the mapping rule for the `IdentityType` column, use the default value **Primary** and enable **Always use default value**.
4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.

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

5. Assign the account definition to employees.

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

Related Topics

- [Setting up account definitions](#) on page 50

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.

- ① **NOTE:** Some administrative user accounts can be automatically identified as privileged user accounts. To do this, enable the **Mark selected user accounts as privileged** schedule in Designer.

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

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

The dummy employee provides the user account with its permissions.

Related Topics

- [Assigning employees with specific permissions to a user account with shared identity](#) on page 80

Privileged User Accounts

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

- ① **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 script TSB_SetIsPrivilegedAccount.

To create privileged users through account definitions

1. Create an account definition. Create a new manage level for privileged user accounts and assign this manage level to the account definition.
2. If you want to prevent the properties for privileged user accounts from being overwritten, set the **IT operating data overwrites** property for the manage level

to **Only initially**. In this case, the properties are populated just once when the user accounts is created.

3. Specify the effect of temporarily or permanently disabling or deleting, or the security risk of an employee on its user accounts and group memberships for each manage level.
4. Create a formatting rule for IT operating data.

You use the mapping rule to define, for example, which rules are used to map the IT operating data for the user accounts, and which default values are used if no IT operating data can be determined via a person's primary roles.

Which IT operating data is required depends on the target system. The following settings are recommended for privileged user accounts:

- In the mapping rule for the `IsPrivilegedAccount` column, use the default value **1** and enable **Always use default value**.
 - You can also specify a mapping rule for the `IdentityType` column. The column owns different permitted values that represent user accounts.
 - To prevent privileged user accounts from inheriting the Entitlements of the default user, define a mapping rule for the `IsGroupAccount` column with a default value of **0** and enable **Always use default value**.
5. Enter the effective IT operating data for the target system.

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

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

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

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

- To use a prefix for the login name, enable the **TargetSystem | EBS | Accounts | PrivilegedAccount | AccountName_Prefix** configuration parameter in Designer.
- To use a postfix for the login name, enable the **TargetSystem | EBS | Accounts | PrivilegedAccount | AccountName_Postfix** configuration parameter in Designer.

These configuration parameters are evaluated in the default installation, if a user account is marked with the property **Privileged user account** (`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.

Related Topics

- [Setting up account definitions](#) on page 50

Assigning employees with specific permissions to a user account with shared identity

Assign employees who use the user account in the target system to an administrative user account with a shared identity. Only employees with the identity **Primary identity** can be assigned.

To assign employees with user permissions

1. Select the category **Oracle E-Business Suite | User accounts**.
2. In the result list, select the user account with a shared identity.
3. Select the task **Assign employees authorized to use**.
4. Assign employees in **Add assignments**.
- OR -
Remove employees from **Remove assignments**.
5. Save the changes.

Provision of login information

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 information generated to users.

Detailed information about this topic

- [Password policies for E-Business Suite user accounts](#) on page 81
- [Initial password for new E-Business Suite user accounts](#) on page 91
- [Email notifications about login data](#) on page 92

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 employees' 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 82
- [Applying password policies](#) on page 83
- [Editing password policies](#) on page 85
- [Custom scripts for password requirements](#) on page 88
- [Editing the exclusion list for passwords](#) on page 90

- [Checking passwords](#) on page 90
- [Testing the generation of passwords](#) on page 91

Predefined password policies

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

Password for logging in to One Identity Manager

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

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

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

Password policy for forming employees' central passwords

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

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

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

Password policies for user accounts

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

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

The **Oracle E-Business Suite password policy** password policy is predefined for 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.

Applying password policies

The **Oracle E-Business Suite password policy** password policy is predefined for 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 account definition of the user account
2. Password policy of the manage level of the user account
3. Password policy for the E-Business Suite system of the user account
4. Password policy **One Identity Manager password policy** (default policy)

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

To reassign a password policy

1. Select **Oracle E-Business Suite | Basic configuration data | Password policies** in Manager.
2. Select the password policy in the result list.
3. Select **Assign objects**.

- Click **Add** in the **Assignments** section and enter the following data.

Table 25: Assigning a Password Policy

Property	Description
Apply to	<p>Application scope of the password policy.</p> <p>To specify an application scope</p> <ol style="list-style-type: none"> Click → next to the text box. Select one of the following references under Table: <ul style="list-style-type: none"> The table that contains the base objects of synchronization. Select the TSBAccountDef table to apply the password policy based on the account definition. Select the TSBBehavior table to apply the password policy based on the manage level. Select the table that contains the base objects under Apply to. <ul style="list-style-type: none"> 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. Click OK.
Password column	The password column's identifier.
password policy	The identifier of the password policy to be used.


- Save the changes.

To change a password policy's assignment

- Select **Oracle E-Business Suite | Basic configuration data | Password policies** in Manager.
- Select the password policy in the result list.
- Select **Assign objects**.
- Select the assignment you want to change in **Assignments**.
- Select the new password policy to apply from the **Password Policies** menu.
- Save the changes.

Editing password policies

To edit a password policy

1. Select **Oracle E-Business Suite | Basic configuration data | Password policies** in Manager.
2. Select the password policy in the result list and select **Change master data**.
- OR -
Click  in the result list toolbar.
3. Edit the password policy's master data.
4. Save the changes.




Detailed information about this topic


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

General master data for a password policy

Enter the following master data for a password policy.

Table 26: Master data for a password policy

Property	Meaning
Display name	Password policy name. Translate the given text using the  button.
Description	Spare text box for additional explanation. Translate the given text using the  button.
Error Message	Custom error message outputted 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.

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

Policy settings

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

Table 27: Policy Settings

Property	Meaning
Initial password	Initial password for newly created user accounts. If a password is not entered or if a random password is not generated when a user account is created, the initial password is used.
Password confirmation	Reconfirm password.
Max. length	Minimum length of the password. Specify the number of characters a password must have.
Max. length	Maximum length of the password. Specify the number of characters a password can have.
Max. errors	<p>Maximum number of errors. Set the number of invalid passwords. Only taken into account when logging in to One Identity Manager.</p> <p>If a user has reached the number of maximum failed logins, the employee or system user can no longer log in to One Identity Manager.</p> <p>You can reset the passwords of employees and system users who have been blocked in Password Reset Portal. For more detailed 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.
Password history	Enter the number of passwords to be saved. If, for example, a value of 5 is entered, the user's last five passwords are stored.
Min. password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value 0 means that the password strength is not tested. The values 1 , 2 , 3 and 4 specify the required complexity of the password. The value 1 represents the lowest requirements in terms of password strength. The value 4 requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted or not permitted in the password. If this option is enabled, name properties are not permitted in passwords. The values of the columns for which the Contains name properties for

Property	Meaning
	password check option is set are taken into account. Adjust this option in the column definition in Designer.

Character classes for passwords

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

Table 28: Character classes for passwords

Property	Meaning
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 characters.
Max. identical characters in total	Maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Maximum number of identical character that can be repeated after each other.
Denied special characters	List of characters, which are not permitted.
Lowercase not allowed	Specifies whether the password can contain lower case letters. This setting is only applies when passwords are generated.
Uppercase not allowed	Specifies whether the password can contain upper case letters. This setting is only applies when passwords are generated.
Digits not allowed	Specifies whether the password can contain digits. This setting is only applies when passwords are generated.
Special characters not allowed	Specifies whether the password can contain special characters. This setting is only applies when passwords are generated.

Custom scripts for password requirements

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

Detailed information about this topic

- [Script for checking a password](#) on page 88
- [Script for generating a password](#) on page 89

Script for checking a password

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

Syntax for Check Scripts

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

With parameters:

policy = password policy object

spwd = password to test

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

Example for a script for testing a password

A password cannot start with ? or !. 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
```



```
        End If
    End If
End Sub
```

To use a custom script for checking a password

1. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
 - a. Select **Oracle E-Business Suite | Basic configuration data | Password policies** in Manager.
 - b. Select the password policy in the result list.
 - c. Select **Change master data**.
 - d. Enter the name of the script to be used to check a password in the **Check script** input field on the **Scripts** tab.
 - e. Save the changes.

Related Topics

- [Script for generating a password](#) on page 89

Script for generating a password

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

Syntax for generating script

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

With parameters:

policy = password policy object

spwd = generated password

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

Example for a script to generate a password

In random passwords, the script replaces the ? and ! characters, which are not permitted.

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

```
    Dim pwd = spwd.ToInsecureArray()
```

```
    ' replace invalid characters at first position
```

```

If pwd.Length>0
    If pwd(0)="?" Or pwd(0)="!"
        spwd.SetAt(0, CChar("_"))
    End If
End If
End Sub

```

To use a custom script for generating a password

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

Related Topics

- [Script for checking a password](#) on page 88

Editing the exclusion list for passwords

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

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

To add a term to the restricted list

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

Checking passwords

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

To test whether a password conforms to the password policy

1. Select **Oracle E-Business Suite | Basic configuration data | Password policies** in Manager.
2. Select the password policy in the result list.
3. Select **Change master data**.
4. Select the **Test** tab.
5. Select the table and object to be tested in **Base object for test**.
6. Enter a password in **Enter password to test**.

A display next to the password shows whether it is valid or not.

Testing 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. Select **Oracle E-Business Suite | Basic configuration data | Password policies** in Manager.
2. Select the password policy in the result list.
3. Select **Change master data**.
4. Select the **Test** tab.
5. Click **Generate**.

This generates and displays a password.

Initial password for new E-Business Suite user accounts

You have the following possible options for issuing an initial password for a new E-Business Suite user account.

- Create user accounts manually and enter a password in their master data.
- Assign a randomly generated initial password to enter when you create user accounts.
 - In the Designer, set the configuration parameter **TargetSystem | EBS | Accounts | InitialRandomPassword**.
 - Apply target system specific password policies and define the character sets

that the password must contain.

- Specify which employee will receive the initial password by email.
- User the employee's central password. The employee's central password is mapped to the user account password. For detailed information about an employee's central password, see *One Identity Manager Identity Management Base Module Administration Guide*.

Related Topics

- [Password policies for E-Business Suite user accounts](#) on page 81
- [Email notifications about login data](#) on page 92

Email notifications about login data

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

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

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

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

To send initial login data by email

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

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

3. In the Designer set the configuration parameter **TargetSystem | EBS | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName**.

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

4. In the Designer, set the configuration parameter **TargetSystem | EBS | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword**.

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

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

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 the 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 authorization assignments for a user account.

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

Table 29: Identification of direct and indirect entitlement assignments in table EBSUserInResp

Assignment origin	Type of assignment	Indirect (Column OriginIndirect)	origin (Column XOrigin)
Oracle E-Business Suite	indirect	1 (yes)	1
	direct	0 (no)	1

Assignment origin	Type of assignment	Indirect (Column OriginIndirect)	origin (Column XOrigin)
One Identity Manager	direct	0 (no)	1
	indirect	0 (no)	2
	Dynamic	0 (no)	4
	assignment request	0 (no)	8
	ineffective	0 (no)	16

For detailed information about the calculation of 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 95
- [Validity period of permission assignments](#) on page 104

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 employees. In the case of indirect assignment, employees and entitlements are organized in hierarchical roles. The number of entitlements assigned to an employee is calculated from the position in the hierarchy and the direction of inheritance. If the employee has an E-Business Suite user account, the entitlements are assigned to this user account. Prerequisites for indirect assignment of employees to user accounts:

- The assignment of employees and E-Business Suite entitlements is permitted for departments, cost centers, locations, or business roles.
- The **Entitlements can be inherited** option is selected for the user accounts.
- The user accounts are linked with an employee via the UID_Person (**Person**) column.
- User accounts and E-Business Suite entitlements belong to the same E-Business Suite system.

Entitlements can also be assigned to employees via IT Shop requests. To enable the assignment of entitlements via IT Shop requests, employees 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 employees.

You can use system roles to group entitlements together and assign them to employees as a package. You can create system roles that contain only E-Business Suite entitlements. System entitlements from different target systems can also be grouped together in a system role.

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

For detailed information see the following guides:

Theme	Guide
Inheritance of 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 via 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 104
- [Assigning E-Business Suite entitlements to departments, cost centers, and locations](#) on page 96
- [Assigning E-Business Suite entitlements to business roles](#) on page 97
- [Assigning E-Business Suite user accounts directly to an entitlement](#) on page 100
- [E-Business Suite Include entitlements in system roles](#) on page 98
- [E-Business Suite Adding entitlements to IT Shop](#) on page 99
- [E-Business Suite Assigning entitlements directly to a user account](#) on page 102

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 via these organizational entities.

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

1. Select **Oracle E-Business Suite | Entitlements**.
2. Select the entitlements in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
 - Assign departments on the **Departments** tab.
 - Assign locations on the **Locations** tab.
 - Assign cost centers on the **Cost centers** tab.

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

To remove an assignment

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

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

1. Select **Organizations | Departments**.
 - OR -
 - Select the category **Organizations | Cost centers**.
 - OR -
 - Select the category **Organizations | Locations**.
2. Select the department, cost center or location in the result list.
3. Select **Assign E-Business Suite entitlements** in the task view.
4. Assign the entitlements in the **Add assignments** area.
 - OR -
 - Remove the entitlements in the **Remove assignments** area.
5. Save the changes.

Related Topics

- [One Identity Manager users for managing an Oracle E-Business Suite](#) on page 9

Assigning E-Business Suite entitlements to business roles

Installed modules: Business Roles Module

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

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

1. Select **Oracle E-Business Suite | Entitlements**.
2. Select the entitlements in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

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

To remove an assignment

- Select the business role and double click .

5. Save the changes.

To assign entitlements to a business role (role-based login):

1. Select the category **Business roles | <Role class>**.
2. Select the business role in the result list.
3. Select **Assign E-Business Suite entitlements** in the task view.
4. Assign the entitlements in the **Add assignments** area.
- OR -
Remove the entitlements in the **Remove assignments** area.
5. Save the changes.

Related Topics

- [One Identity Manager users for managing an Oracle E-Business Suite](#) on page 9

E-Business Suite Include entitlements in system roles

Installed modules: System Roles Module

Use this task to add an entitlement to system roles. When you assign a system role to an employee, the entitlement is inherited by all user accounts of this employee.

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

To assign a group to system roles:

1. Select **Oracle E-Business Suite | Entitlements**.
2. Select the entitlements in the result list.
3. Select **Assign system roles**.
4. Assign system roles in **Add assignments**.

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

To remove an assignment

- Select the system role and double click .

5. Save the changes.

E-Business Suite Adding entitlements to IT Shop

When you assign a permission to a IT Shop shelf, it can be requested by the shop customers. To ensure it can be requested, further prerequisites need to be guaranteed.

- the permission must be marked with the **IT Shop** option.
- the permission must be assigned a service item.

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

- If you only want it to be possible for the permission to be assigned to employees through IT Shop requests, the permission 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 IT Shop.

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

4. In **Add assignments**, the entitlement to the IT Shop shelves.
5. Save the changes.

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

1. In Manager, select **Oracle E-Business Suite | Entitlements** (non-role-based login).
- OR -
In Manager, select **Entitlements | E-Business Suite Entitlements** (role-based login).
2. In the result list, select the permission.
3. Select **Add to IT Shop**.
4. In **Remove assignments**, the entitlement from the IT Shop shelves.
5. Save the changes.

To remove, an entitlement from all shelves of the IT Shop

1. In Manager, select **Oracle E-Business Suite | Entitlements** (non-role-based login).
- OR -
In Manager, select **Entitlements | E-Business Suite Entitlements** (role-based login).
2. In the result list, select the permission.
3. Select **Remove from all shelves (IT Shop)**.
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 detailed information about requesting company resources through IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Related Topics

- [General master data for E-Business Suite entitlements](#) on page 125
- [One Identity Manager users for managing an Oracle E-Business Suite](#) on page 9

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. Select **Oracle E-Business Suite | Entitlements**.
2. Select the entitlements in the result list.
3. Select **Assign user accounts**.

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** menu.
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 XOrigin is assigned the value **16**.

Detailed information about this topic

- [Validity period of permission assignments](#) on page 104

Related Topics

- [Invalid entitlement assignments](#) on page 110

E-Business Suite Assigning entitlements directly to a user account

To enable a quick response to special requests, you can assign entitlements directly to a user account.

To assign entitlements directly to a user account

1. Select the category **Oracle E-Business Suite | User accounts**.
2. Select the user account in the result list.
3. Select **Assign entitlements**.

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** menu.
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 104

Related Topics

- [Invalid entitlement assignments](#) on page 110
- [E-Business Suite Adding entitlements to IT Shop](#) on page 99

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. The 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 30: Properties of a permission assignment

Property	Description
Active from (effective)	First date from which the assignment is valid. This date is calculated from 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 the One Identity Manager.
Description	Spare text box 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. The One Identity Manager calculates the effective validity period from all the assignments. The different assignment types are incorporated into the calculation as follows:

Table 31: Determine validity period

Type of assignment	Validity period
Direct assignment	Active from (direct) and Active to (direct)
Request	Validity period of the request when the Valid from 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 Valid from date of the request has been reached or exceeded. For unlimited requests, 01.01.1900 is entered at the first validity date.
Inheritance via 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 The date of the assignment is set as the first date of the validity.
Inheritance via 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 95

Related Topics

- [Invalid entitlement assignments](#) on page 110

Effectiveness of entitlement assignments

When E-Business Suite entitlements are assigned to user accounts an employee may obtain two or more groups, which are not permitted in this combination. To prevent this, you can declare mutually exclusive 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.

i 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 department "Marketing", entitlement B through "Finance", and entitlement C through the business role "Control group".

Clara Harris has a user account in this system. She primarily belongs to the department "marketing". The business role "Control group" and the department "Finance" are assigned to her secondarily. Without an exclusion definition, the user account obtains all the entitlements A, B and C.

You need to use a suitable method to ensure that a employee cannot be assigned the 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 32: Definition of excluded entitlements (table EBSRespExclusion)

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

Table 33: Effective Assignments

Employee	Member in Role	Effective entitlement
Ben King	Marketing	Entitlement A
Jan Bloggs	Marketing, finance	Entitlement B
Clara Harris	Marketing, finance, control group	Entitlement C
Jenny Basset	Marketing, control group	Entitlement A Entitlement C

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

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

Table 34: Excluded entitlements and effective assignments

Employee	Member in Role	Assigned entitlement	Excluded entitlement	Effective entitlement
Jenny Basset	Marketing	Entitlement A		Entitlement C
	Control group	Entitlement C	Entitlement B Entitlement A	

Prerequisites

- The configuration parameter **QER | Structures | Inherit | GroupExclusion** is enabled.
- Mutually exclusive entitlements belong to the same E-Business Suite system.

To exclude entitlements

1. Select **Oracle E-Business Suite | Entitlements**.
2. Select an entitlement in the result list.
3. Select **Exclude E-Business Suite entitlements** in the task view.
4. In the **Add assignments** area, assign the entitlements that are excluded by the selected entitlement.

- OR -

In the **Remove assignments** area, delete the entitlements that no longer exclude each other.

5. Save the changes.

Related Topics

- [Invalid entitlement assignments](#) on page 110

Inheritance of E-Business Suite entitlements based on categories

In One Identity Manager, entitlements can be selectively inherited by user accounts. For this purpose, the entitlements and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within this mapping rule. 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 31**.

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.

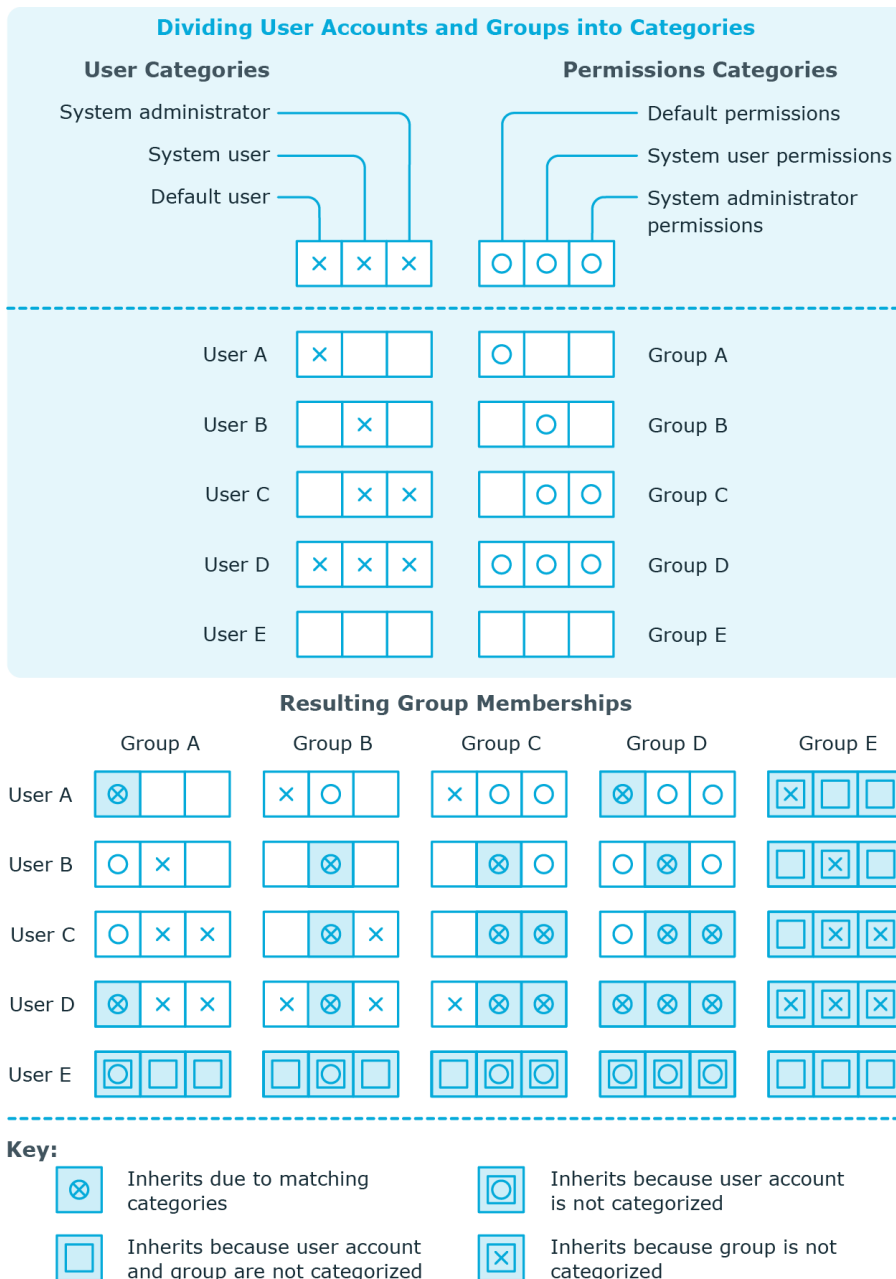
NOTE: Inheritance through categories is only taken into account when entitlements are assigned indirectly via hierarchical roles. Categories are not taken into account when entitlements are directly assigned to user accounts.

Table 35: Category Examples

Category Position	Categories for User Accounts	Categories for entitlements
1	Default user	Default entitlements

Category Position	Categories for User Accounts	Categories for entitlements
2	System user	System user entitlements
3	System administrator	System administrator entitlements

Figure 2: Example of inheriting through categories.



To use inheritance through categories

- Define the categories in the E-Business Suite system.
- Assign categories to user accounts through their master data.
- Assign categories to entitlements through their master data.

Related Topics

- [Defining categories for the inheritance of E-Business Suite entitlements](#) on page 115
- [General master data for E-Business Suite user accounts](#) on page 117
- [General master data for E-Business Suite entitlements](#) on page 125

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 employees and handling of user accounts via an account definition

For user accounts with the manage level **Full managed**, the account definition defines how entitlement assignments are handled if the employee is classified as a security risk, or the employee 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 via 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 the value **16**.

If the cause of an 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 106
- [Master data for manage levels](#) on page 54
- [Master data for account definitions](#) on page 51
- [Assigning E-Business Suite entitlements to departments, cost centers, and locations](#) on page 96
- [Assigning E-Business Suite entitlements to business roles](#) on page 97
- [E-Business Suite Include entitlements in system roles](#) on page 98
- [Inheritance of E-Business Suite entitlements based on categories](#) on page 108


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 employees who own the selected base object. In this case, direct as well as indirect base object assignments are included.

Example

- If the report is created for a resource, all roles are determined in which there are employees with this resource.
- If the report is created for a group or another system entitlement, all roles are determined in which there are employees with this group or system entitlement.
- If the report is created for a compliance rule, all roles are determined in which there are employees with this compliance rule.
- If the report is created for a department, all roles are determined in which employees of the selected department are also members.
- If the report is created for a business role, all roles are determined in which employees of the selected business role are also members.

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the report **Overview of all assignments**.
- Click the  **Used by** button in the report toolbar to select the role class for which you want to determine whether roles exist that contain employees with the selected base object.

All the roles of the selected role class are shown. The color coding of elements identifies the role in which there are employees with the selected base object. The meaning of the report control elements is explained in a separate legend. To access the legend, click the  icon in the report's toolbar.



- Double-click a control to show all child roles belonging to the selected role.
- By clicking the  button in a role's control, you display all employees in the role with the base object.
- Use the small arrow next to  to start a wizard that allows you to bookmark this list of employee for tracking. This creates a new business role to which the employees are assigned.

Figure 3: Toolbar of the Overview of all assignments report.

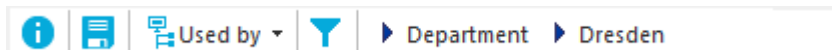






Table 36: Meaning of Icons in the Report Toolbar

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 of 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 are required for the configuration of provisioning processes, the automatic assignment of employees to user accounts, and the inheritance of permissions to user accounts within an Oracle E-Business Suite.

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

To set up a system:

1. Select the category **Oracle E-Business Suite | Systems**.
2. Select the system in the result list. Select **Change master data**.
3. Edit the master data for the system.
4. Save the changes.

General master data for E-Business Suite systems

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

Table 37: General master data for 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 employees to user accounts is used for this system and if user accounts are to be created that are already managed (Linked configured). The account definition's default manage level is applied.</p> <p>User accounts are only linked to the employee (Linked) 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 the 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, One Identity Manager is used.</p>

Table 38: 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 65
- [Setting up account definitions](#) on page 50
- [Automatic assignment of employees to E-Business Suite user accounts](#) on page 67
- [Target system managers](#) on page 146

Defining categories for the inheritance of E-Business Suite entitlements

In One Identity Manager, entitlements can be selectively inherited by user accounts. For this purpose, the entitlements and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within this mapping rule. 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 31**.

To define a category

1. In Manager, select the system in **Oracle E-Business Suite | Systems**.
2. Select **Change master data**.
3. Switch to the **Mapping rule category** tab.
4. Extend the relevant roots of a table.
5. Click  to enable category.
6. Enter a category name of your choice for user accounts and entitlements and in the login language used.
7. Save the changes.

Detailed information about this topic

- [Inheritance of E-Business Suite entitlements based on categories](#) on page 108

Editing a synchronization project

Synchronization projects in which a system is already used as a base object can also be opened via 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 Manager, select **Oracle E-Business Suite | Systems**.
2. Select the system in the result list.
3. Select **Change master data**.
4. Select **Edit synchronization project**.

Related Topics

- [Customizing synchronization configuration](#) on page 25

E-Business Suite User accounts

You use One Identity Manager to manage the user accounts of an Oracle E-Business Suite. A user can log on to the Oracle E-Business Suite using their 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 employees who are managed in the Oracle E-Business Suite. Employee 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 employee in One Identity Manager. You can also manage user accounts separately from employees.


- NOTE:** It is recommended to use account definitions to set up user accounts for company employees. In this case, some of the master data described in the following is mapped through templates from employee master data.
- NOTE:** If employees are to obtain their user accounts through account definitions, the employees must own a 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 employees](#) on page 49
- [Setting up account definitions](#) on page 50
- [Appendix: Default project templates for synchronizing an Oracle E-Business Suite](#) on page 151
- [Entering master data for E-Business Suite user accounts](#) on page 117

Entering master data for E-Business Suite user accounts

To create a user account

1. In Manager, select **Oracle E-Business Suite | User accounts**.
2. Click  in the result list toolbar.
3. On the master data form, edit the master data for the user account.
4. Save the changes.

To edit master data for a user account

1. In Manager, select **Oracle E-Business Suite | User accounts**.
2. Select the user account in the result list and run **Change master data**.
3. Edit the user account's resource data.
4. Save the changes.


Detailed information about this topic

- [General master data for E-Business Suite user accounts](#) on page 117
- [Login data for E-Business Suite user accounts](#) on page 121

General master data for E-Business Suite user accounts

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

Table 39: Additional Master Data for a User Account

Property	Description
Employee	<p>Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. If you are using automatic employee assignment, an associated employee is found and added to the user account when you save the user account.</p> <p>For a user account with an identity of type Organizational identity, Personalized administrator identity, Sponsored identity, Shared identity or Service identity, you can create a new employee. To do this, click  next to the input field and enter the required employee master data. Which login data is required depends on the selected identity type.</p>

Property	Description
	<p>i NOTE: To enable working with identities for user accounts, the employees also need identities. You can only link user accounts to which an identity is assigned with employees who have this same identity.</p>
Account definition	<p>Account definition through which the user account was created.</p> <p>Use the account definition to automatically fill user account master data and to specify a manage level for the user account. The One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account.</p> <p>i NOTE: The account definition cannot be changed once the user account has been saved.</p>
Manage level	<p>Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.</p>
User name	<p>User account identifier. If you have assigned an account definition, this input field is filled automatically depending on the manage level.</p>
Display name	<p>User account display name. If you have assigned an account definition, this input field is filled automatically depending on the manage level.</p>
Distinguished name	<p>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.</p>
Email address	<p>User account email address. If you have assigned an account definition, this input field is filled automatically depending on the manage level.</p>
Fax	<p>Fax number for the user account. If you have assigned an account definition, this input field is filled automatically depending on the manage level.</p>
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 (Active from (date), Active to (date)).</p>

Status	Meaning
--------	---------

ACTIVE	The current date is within the validity period.
INACTIVE	<ul style="list-style-type: none"> The active-from date has not yet been reached or the active-to date is in the past. The user account has been deleted.

Property	Description
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 Suitesystem	E-Business Suitesystem in which you want to create the user account.
Customer	Reference to an employee who is managed as a customer. Only employees from the E-Business Suite AR data source can be assigned (Person.ImportSource='EBSOIM').
HR employee	Reference to an employee in the Human Resources module of Oracle E-Business Suite. Only employees from the E-Business Suite HR data source can be assigned (Person.ImportSource='EBSHR').
Party	Reference to an employee who is managed as a party. An employee with the E-Business Suite AR data source can be assigned (Person.ImportSource='EBSOIM'). The assignment cannot be edited in One Identity Manager.
Supplier	Reference to an employee who is managed as a supplier or a contact. Only employees from the E-Business Suite AP data source can be assigned (Person.ImportSource='EBSCRM').
Risk index (calculated)	Maximum risk index value of all assigned entitlements. The property is only visible if the QER CalculateRiskIndex configuration parameter is enabled. For more detailed information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Category	Categories for the inheritance of E-Business Suite entitlements to the user account. User accounts can selectively inherit entitlements. To do this, entitlements and user accounts are divided into categories. Select one or more categories from the menu.
Description	Spare text box for additional explanation.
Identity	User account's identity type Permitted values are: <ul style="list-style-type: none"> • Primary identity: Employee's default user account. • Organizational identity: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.

Property	Description
	<ul style="list-style-type: none"> • Personalized administrator identity: User account with administrative entitlements, used by one employee. • Sponsored identity: User account that is used for training purposes, for example. • Shared identity: User account with administrative entitlements, used by several employees. Assign all employees show use the user account. • Service identity: Service account.
Privileged user account	Specifies whether this is a privileged user account.
Entitlements can be inherited	<p>Specifies whether the user account may inherit E-Business Suite entitlements via the employee. If this option is set, the user account inherits entitlements through hierarchical roles or IT Shop requests.</p> <ol style="list-style-type: none"> 1. Example: An employee 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. 2. Example: An employee with an E-Business Suite user account requests a G Suite entitlement in the IT Shop. The request is approved and assigned. The user account only inherits this entitlement if this option is active.
User account is disabled	Specifies whether the user account is blocked from logging in to the E-Business Suite system. The status of the user account is transferred via a template. To disable the user account, edit the last validity date of the user account.

Related Topics

- [Managing E-Business Suite user accounts and employees](#) on page 49
- [Setting up account definitions](#) on page 50
- [Automatic assignment of employees to E-Business Suite user accounts](#) on page 67
- [Inheritance of E-Business Suite entitlements based on categories](#) on page 108
- [E-Business Suite Disabling user accounts](#) on page 123
- [Linking E-Business Suite user accounts to imported employees](#) on page 73
- [Supported user account types](#) on page 75
- [Assigning employees with specific permissions to a user account with shared identity](#) on page 80

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 the One Identity Manager it cannot be changed.

Table 40: Login data for a user account

Property	Description
Last login	Date of last login.
Password	Password for the user account. Based on the QER Person UseCentralPassword configuration parameter, the central password of the assigned employee is mapped to the password of the user account. If you use an initial password for the user accounts, it is automatically entered when a user account is created. NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements.
Confirmation	Reconfirm password.
Logins (remaining)	Number of logins remaining until the password expires.
Password last changed	Date 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 91

Additional tasks for managing E-Business Suite user accounts

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Task	Theme
Overview of E-Business Suite User Accounts	Overview of E-Business Suite user accounts on page 122

Task	Theme
Assigning Permissions	E-Business Suite Assigning entitlements directly to a user account on page 102
Assigning extended properties	Assigning extended properties to an E-Business Suite user account on page 122
Assign employees with user permissions	Assigning employees with specific permissions to a user account with shared identity on page 80

Overview of E-Business Suite user accounts

To obtain an overview of a user account

1. Select **Oracle E-Business Suite | User accounts**.
2. Select the user account in the result list.
3. Select **E-Business Suite user account overview**.

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

Assigning extended properties to an E-Business Suite user account

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

To specify extended properties for a user account

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

For detailed information about extended properties, see the *One Identity Manager Identity Management Base Module Administration Guide*.

E-Business Suite Disabling user accounts

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

Scenario:

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

User accounts managed through account definitions are disabled when the employee is temporarily or permanently disabled. The behavior depends on the user account manage level. Accounts with the manage level **Full managed** manage level are disabled depending on the account definition settings. For user accounts with a manage level, configure the required behavior using the template in the `EBSUser.EndDatePAGUser.IsDisabled` column.

Scenario:

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

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

- If the configuration parameter is set, the employee's user accounts are disabled if the employee is permanently or temporarily disabled.
- If the configuration parameter is not set, the employee'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 Manager, select **Oracle E-Business Suite | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data**.
4. Enter the current date in the **Active to (date)** input field on the **General** tab.
The status of the user account is set to **INACTIVE**.
5. Save the changes.

Scenario:

- User accounts not linked to employees.

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

1. In Manager, select **Oracle E-Business Suite | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data**.
4. Enter the current date in the **Active to (date)** input field on the **General** tab.

The status of the user account is set to **INACTIVE**.

5. Save the changes.

To activate a user account

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

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

Related Topics

- [Setting up account definitions](#) on page 50
- [Creating manage levels](#) on page 53
- [Deleting E-Business Suite user accounts](#) on page 124

Deleting E-Business Suite user accounts

E-Business Suite user accounts in One Identity Manager cannot be physically deleted. If a user account is deleted via 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)**).

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

Related Topics


- [E-Business Suite Disabling user accounts](#) on page 123

E-Business Suite entitlements

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 master data for E-Business Suite entitlements

To edit the master data of an entitlement:

1. Select **Oracle E-Business Suite | Entitlements**.
2. To edit an entitlement, select the entitlement in the result list and execute **Change master data**.
- OR -
To create a new entitlement, click  in the result list
This opens the master data form for an E-Business Suite entitlement.
3. Edit the master data for the entitlement.
4. Save the changes.

Detailed information about this topic

- [General master data for E-Business Suite entitlements](#) on page 125

General master data for E-Business Suite entitlements

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

Table 41: General master data for 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 entitlements. To do this, entitlements and user accounts are divided into categories. Select one or more categories from the menu.
Risk index	Value for evaluating the risk of assigning the entitlement to user accounts. Enter a value between 0 and 1 . This input field is only visible if

Property	Description
	the configuration parameter QER CalculateRiskIndex is activated. For detailed information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Service item	Service item for requesting the entitlement via 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 granted using a defined approval process. 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 granted using a defined approval process. 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 108
- [E-Business Suite Adding entitlements to IT Shop](#) on page 99

Additional tasks for managing E-Business Suite entitlements

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Task	Theme
Overview of E-Business Suite entitlements	Overview of E-Business Suite entitlements on page 127
assign user accounts	Assigning E-Business Suite user accounts directly to an entitlement on page 100
Assigning extended properties	Assigning extended properties to an E-Business Suite entitlement on page 127
Exclude E-Business Suite entitlements	Effectiveness of entitlement assignments on page 106
Assign system roles	E-Business Suite Include entitlements in system roles on page 98
Assign business roles	Assigning E-Business Suite entitlements to business roles on page 97

Task	Theme
Assign organizations	Assigning E-Business Suite entitlements to departments, cost centers, and locations on page 96
Add to IT Shop	E-Business Suite Adding entitlements to IT Shop on page 99

Overview of E-Business Suite entitlements

To obtain an overview of entitlements

1. Select **Oracle E-Business Suite | Entitlements**.
2. Select the entitlements in the result list.
3. Select **E-Business Suite entitlements overview** in the task view.

Assigning extended properties to an E-Business Suite entitlement

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

To specify extended properties for an entitlement

1. Select **Oracle E-Business Suite | Entitlements**.
2. Select the E-Business Suite entitlement in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.
- OR -
Remove extended properties from **Remove assignments**.
5. Save the changes.

E-Business Suite applications

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

To display the properties of an application:

1. Select **Oracle E-Business Suite | Hierarchical view | <E-Business Suite System> | Applications**.
2. Select the application in the result list.
3. Select **Change master data**.

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

To obtain an overview of an application:

1. Select **Oracle E-Business Suite | Hierarchical view | <E-Business Suite System> | Applications**.
2. Select the application in the result list.
3. Select **E-Business Suite application overview**.

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 their properties.

To display the properties of a menu:

1. Select the category **Oracle E-Business Suite | Hierarchical view | <E-Business Suite System> | Menus**.
2. Select the menu in the result list.
3. Select **Change master data**.

Menus are assigned to user accounts via 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. Select the category **Oracle E-Business Suite | Hierarchical view | <E-Business Suite System> | Menus**.
2. Select the menu in the result list.
3. Select **E-Business Suite menu overview** in the task view.

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 via the assignment to E-Business Suite responsibilities. Data groups are imported into the One Identity Manager database during synchronization. You cannot edit their properties.

To display the properties of a data group:

1. Select **Oracle E-Business Suite | Hierarchical view | <E-Business Suite System> | Data groups**.
2. Select the data group in the result list.
3. Select **Change master data**.

To obtain an overview of a data group:

1. Select **Oracle E-Business Suite | Hierarchical view | <E-Business Suite System> | Data groups**.
2. Select the data group in the result list.
3. Select **E-Business Suite data group overview**.

E-Business Suite Data group units

Data groups are assigned to E-Business Suite applications in E-Business Suite data group units. 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. Select **Oracle E-Business Suite | Hierarchical view | <E-Business Suite System> | Applications | <Application> | Data group units**.
2. Select the data group unit in the result list.
3. Select **Change master data**.

To obtain an overview of a data group unit:

1. Select **Oracle E-Business Suite | Hierarchical view | <E-Business Suite System> | Applications | <Application> | Data group units**.
2. Select the data group unit in the result list.
3. Select **E-Business Suite data group unit overview**.

E-Business Suite Request groups

E-Business Suite request groups can be used to assign permissions for the execution of 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 their properties.

To display the properties of a request group:

1. Select **Oracle E-Business Suite | Hierarchical view | <E-Business Suite System> | Applications | <Application> | Request groups**.
2. Select the request group in the result list.
3. Select **Change master data**.

To obtain an overview of a request group:

1. Select **Oracle E-Business Suite | Hierarchical view | <E-Business Suite System> | Applications | <Application> | Request groups**.
2. Select the request group in the result list.
3. Select **E-Business Suite request group overview** in the task view.

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 their properties.

To display the properties of a security group:

1. Select the category **Oracle E-Business Suite | Hierarchical view | <E-Business Suite system> | Security groups**.
2. Select the security group in the result list.
3. Select **Change master data**.

To obtain an overview of a security group:

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

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 their properties.

To display the properties of an attribute:

1. Select **Oracle E-Business Suite | Hierarchical view | <E-Business Suite System> | Applications | <Application> | Attributes**.
2. Select the attribute in the result list.
3. Select **Change master data**.

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. Select **Oracle E-Business Suite | Hierarchical view | <E-Business Suite System> | Applications | <Application> | Attributes**.
2. Select the attribute in the result list.
3. Select **E-Business Suite attribute overview** in the task view.

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

E-Business Suite responsibilities

E-Business Suite responsibilities control the access rights 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 their 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.

Displaying master data for E-Business Suite responsibilities

To display the properties of a responsibility:

1. Select **Oracle E-Business Suite | Hierarchical view | <E-Business Suite System> | Applications | <Application> | Responsibilities.**
2. Select the responsibility in the result list.
3. Select **Change master data.**

To obtain an overview of a responsibility:

1. Select **Oracle E-Business Suite | Hierarchical view | <E-Business Suite System> | Applications | <Application> | Responsibilities.**
2. Select the responsibility in the result list.
3. Select the task **E-Business Suite responsibility overview.**

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

Detailed information about this topic

- [General master data for E-Business Suite responsibilities](#) on page 132

General master data for E-Business Suite responsibilities

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

Table 42: General master data for 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 (date)	First date on which the responsibility is valid.
Valid to (date)	Last date on which the responsibility is valid

Property	Description
	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"> • AOL (Oracle Applications) • Web (Oracle Self-Service Web Applications) • Mobile (Oracle Mobile Applications) • Direct Access • None
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. Select the category **Oracle E-Business Suite | HR people**.
2. Select the employee in the result list.
3. Select **Change master data**.

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

4. Select **Employee overview** in the task view.

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

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

The following employee master 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 master data in the usual way. For more detailed information about editing employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

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

Related Topics

- [Linking E-Business Suite user accounts to imported employees](#) on page 73
- [General master data for E-Business Suite user accounts](#) on page 117
- [Setting up a synchronization project for employee data](#) on page 23
- [Project templates for HR data](#) on page 152

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. Select **Oracle E-Business Suite | Suppliers and contacts**.
2. Select the employee in the result list.

3. Select **Change master data**.

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

4. Select **Employee overview** in the task view.

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

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

The following employee master 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 master data in the usual way. For more detailed information about editing employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

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

Related Topics

- [Linking E-Business Suite user accounts to imported employees](#) on page 73
- [General master data for E-Business Suite user accounts](#) on page 117
- [Setting up a synchronization project for organizational data](#) on page 24
- [Project templates for CRM data](#) on page 153

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 via the synchronization.

To display the properties of a party:

1. Select the category **Oracle E-Business Suite | Parties**.
2. Select the employee in the result list.
3. Select **Change master data**.

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

4. Select **Employee overview** in the task view.

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

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

The following employee master 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 master data in the usual way. For more detailed information about editing employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

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

Related Topics

- [Linking E-Business Suite user accounts to imported employees](#) on page 73
- [General master data for E-Business Suite user accounts](#) on page 117
- [Setting up a synchronization project for organizational data](#) on page 24
- [Project template for OIM data](#) on page 153

Locations

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

To display locations that originate from the HR data import:

- Select the category **Organizations | Locations | Data source | E-Business Suite HR**.

The master 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 master data:

- Location
- Description
- Street
- City
- Country

You can maintain all other master data in the usual way. For detailed 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 employee data](#) on page 23
- [Project templates for HR data](#) on page 152

E-Business Suite object reports

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 43: Reports for the Target System

Report	Description
Overview of all assignments (system)	This report finds all roles containing employees with at least one user account in the selected system.
Overview of all assignments (permission)	This report finds all roles containing employees who have the selected permission.
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 category My One Identity Manager Target system overviews .
Show unused user accounts	This report shows all user accounts in the selected system that have not been used in the last few months. The report contains group memberships and risk assessment. You can find the report in the category My One Identity Manager Data quality analysis .
Show entitlement drifts	This report shows all permissions in the selected system that are the result of manual operations in the target system rather than using One Identity Manager. You can find the report in the category My One Identity Manager Data quality analysis .
Show user accounts with an above average number of system entitlements	This report contains all the user accounts in the selected system with an above average number of assigned permissions. You can find the report in the category My One Identity Manager Data quality analysis .
Show orphaned user accounts	This report contains all orphaned user accounts in the selected system, including their assigned entitlements. You can find the report in the category My One Identity Manager Data quality analysis .
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 category My One Identity Manager Data quality analysis .

Handling of E-Business Suite objects in Web Portal

One Identity Manager enables its users to perform various tasks simply using a Web Portal. The Web Portal supports the administration of Oracle E-Business Suite for the following tasks:

- Managing user accounts and employees

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

- Managing entitlement assignments

When aE-Business Suite entitlement is assigned to an IT Shop shelf, the entitlement can be requested by the shop customers in the Web Portal. The request undergoes a defined approval procedure. The entitlement is not assigned until it has been approved by an authorized person.

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 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 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 Manager. The attesters 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 Manager. Supervisors use the Web Portal to check and resolve 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 Manager. Supervisors use the Web Portal to check policy violations and 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. The 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 employees, user accounts, and their entitlements and risks.

For detailed information about the named topics, see [Assigning E-Business Suite entitlements to user accounts in One Identity Manager](#) on page 95 and in 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 employees during working hours. You can create account definitions for every target system. If an employee does not yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

For more information, see [Setting up account definitions](#) on page 50.

- Password policies

One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password 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 81.

- Target system types

Target system types are required for configuring target system comparisons. Tables containing outstanding objects are maintained on target system types.

For more information, see [Post-processing outstanding objects](#) on page 45.

- Server

In order to handle Oracle E-Business Suite -specific processes in One Identity Manager, the synchronization server and its server functions must be declared.

For more information, see [Job server for E-Business Suite-specific process handling](#) on page 142.

- Target system managers

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

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

For more information, see [Target system managers](#) on page 146.

Job server for E-Business Suite-specific process handling

In order to handle Oracle E-Business Suite -specific processes in One Identity Manager, the synchronization server and its server functions must be declared. You have several options for defining a server's functionality:

- Create an entry for the Job server in Designer under **Base Data | Installation | Job server**. For detailed information, see the *One Identity Manager Configuration Guide*.
- Select an entry for the Job server in **Oracle E-Business Suite | Basic configuration data | Server** in Manager and edit the Job server master data.

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

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

Related Topics

- [System requirements for the synchronization server](#) on page 15

Editing E-Business Suite Job servers

To edit a Job server and its functions

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

Detailed information about this topic

- [General master data for Job servers](#) on page 143
- [Specifying server functions](#) on page 145

General master data for Job servers

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

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

Table 44: Job Server Properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Example: <Name of servers>.<Fully qualified domain name>
Target system	Computer account target system.
Language	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The properties Server is cluster and Server belongs to cluster are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the Robocopy and rsync programs are supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed

Property Meaning

	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	<p>Name of the executing server. The name of the server that exists physically and where the processes are handled.</p> <p>This input is evaluated when 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.</p>
Queue	Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values Win32 , Windows , Linux and Unix are permitted. If no value is specified, Win32 is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server) the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain and the service account password have to be entered for the server.
One Identity Manager Service installed	<p>Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the procedure QBM_PJobQueueLoad 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	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.

Property	Meaning
Service	You can make the service start and stop with the appropriate administrative permissions in the program "Job Queue Info". For more detailed information, see the <i>One Identity Manager Process Monitoring and Troubleshooting Guide</i> .
No automatic software update	Specifies whether to exclude the server from automatic software updating. i NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently being executed.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled depending on the server function.

Related Topics

- [Specifying server functions](#) on page 145

Specifying server functions

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

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

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

Table 45: Permitted server functions

Server function	Remark
Update Server	This server executes automatic software updating of all other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. The server can execute SQL tasks. The server with the installed One Identity Manager database, is labeled with this functionality during initial installation of the schema.
SQL processing server	The server can execute SQL tasks. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.

Server function	Remark
CSV script server	The server can process CSV files using the ScriptComponent process component.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
Oracle E-Business Suite connector	Server on which the Oracle E-Business Suite connector is installed. This server executes synchronization with the target system Oracle E-Business Suite.

Related Topics

- [General master data for Job servers](#) on page 143

Target system managers

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

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

For detailed information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Implementing application roles for target system managers

1. The One Identity Manager administrator assigns employees to be target system managers.
2. These target system managers add employees to the default application role for

target system managers.

Target system managers with the default application role are authorized to edit all E-Business Suite systems in One Identity Manager.

3. Target system managers can authorize other employees within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual E-Business Suite systems.

Table 46: Default Application Roles for Target System Managers

Users	Tasks
target system managers	<p>Target system managers must be assigned to Target systems Oracle E-Business Suite or a sub-application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Assume administrative tasks for the target system.• Create, change or delete target system objects, like user accounts or groups.• Edit password policies for the target system.• Prepare entitlements for adding to the IT Shop.• Can create employees with an identity that differs from the Primary identity.• Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager.• Edit the synchronization's target system types and outstanding objects.• Authorize other employees within their area of responsibility as target system managers and create child application roles if required.

To initially specify employees to be target system administrators

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

To add the first employees to the default application as target system managers.

1. Log yourself into Manager as target system administrator (**Target systems | Administrators**).
2. Select **One Identity Manager Administration | Target systems | Oracle E-Business Suite**.
3. Select **Assign employees** in the task view.
4. Assign the employees you want and save the changes.

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

1. Login to Manager as target system manager.
2. Select the application role in Oracle E-Business Suite | **Basic configuration data | Target system managers**.
3. Select **Assign employees**.
4. Assign the employees you want and save the changes.

To specify target system managers for individual E-Business Suite systems

1. Login to Manager as target system manager.
2. Select **Oracle E-Business Suite | Systems**.
3. Select the system in the result list.
4. Select **Change master data**.
5. On the **General** tab, select the application role in the **Target system manager** menu.

- OR -

Next to the **Target system manager** menu, click  to create a new application role.

- a. Enter the application role name and assign the **Target systems | Oracle E-Business Suite** parent application role.
 - b. Click **OK** to add the new application role.
6. Save the changes.
 7. Assign employees to this application role who are permitted to edit the system in One Identity Manager.

Related Topics

- [One Identity Manager users for managing an Oracle E-Business Suite](#) on page 9
- [General master data for E-Business Suite systems](#) on page 113

Appendix: Access rights required for synchronization with an 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.

Tables and views with Select entitlements

- ak.ak_attributes_tl
- ak.ak_excluded_items
- ak.ak_resp_security_attr_values
- ak.ak_web_user_sec_attr_values
- applsys.fnd_application
- applsys.fnd_application_tl
- applsys.fnd_data_groups
- applsys.fnd_data_group_units
- applsys.fnd_languages
- applsys.fnd_menus
- applsys.fnd_menus_tl
- applsys.fnd_request_groups
- applsys.fnd_resp_functions
- applsys.fnd_responsibility
- applsys.fnd_responsibility_tl
- applsys.fnd_security_groups
- 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

Tables with select permissions for synchronizing people data

- ap.ap_supplier_contacts
- ar.hz_parties
- hr.hr_locations_all
- hr.per_all_assignments_f
- hr.per_all_people_f
- hr.per_job_groups
- hr.per_jobs
- hr.per_roles

Tables with Select entitlements for schema types that are created in the connector schema, but are not contained in the default mapping

- applsys.fnd_request_group_units
- applsys.fnd_request_sets
- applsys.fnd_request_sets_tl
- applsys.fnd_user_preferences
- apps.fnd_preferences

Stored procedures with execute permissions

- 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

Appendix: 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 151
- [Project templates for HR data](#) on page 152
- [Project templates for CRM data](#) on page 153
- [Project template for OIM data](#) on page 153

Project template for user accounts and entitlements

For the synchronization of user accounts and entitlements of an Oracle E-Business Suite, you use the project template **Oracle E-Business Suite Synchronization**. The template uses mappings for the following schema types.

Table 47: 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 templates for HR data

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

Table 48: 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	Employee

Schema Type in the Target System	Table in the One Identity Manager Schema
HRPersonManager	Employee
HRLocations	Locality
HRPersonInLocation	PersonInLocality
HRPersonPrimaryLocation	Employee

Project templates 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 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
APSupplierContacts	Employee

Project template for OIM data

For the synchronization of party person data of an Oracle E-Business Suite, you use the project template **Oracle E-Business Suite OIM data**. The 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
HZParty	Employee

Appendix: Editing system objects

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

Table 51: Methods available for editing schema types

Schema type	Read	Insert	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

Schema type	Read	Insert	Delete	Refresh
User account: assignment to responsibility(ORA-UserInRESPIndirect)	Yes	No	No	No
Person (APSupplierContacts)	Yes	No	No	No
Person (HZParty)	Yes	No	No	No
Person (HRPerson)	Yes	No	No	No
Person (HRPersonManager)	Yes	No	No	No
Location (HRLocations)	Yes	No	No	No
Secondary assignment: location (HRPersonInLocation)	Yes	No	No	No

Appendix: 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 52: Configuration parameter

Configuration parameter	Meaning
TargetSystem EBS	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the target system Oracle E-Business Suite. If the parameter is set, the target system components are available. Changes to the parameter require recompiling the database.
TargetSystem EBS Accounts	Parameter for configuring E-Business Suite user account data.
TargetSystem EBS Accounts InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem EBS Accounts InitialRandomPassword SendTo	Specifies to which employee the email with the random generated password should be sent (manager cost center-/department/location/role, employee's manager or XUserInserted). If no recipient can be found, the email is sent to the address stored in the configuration parameter TargetSystem EBS DefaultAddress .
TargetSystem EBS Accounts InitialRandomPassword SendTo MailTemplateName	This configuration parameter contains the name of the mail template sent to provide users with the login data for their user accounts. The Employee - new user account created mail template is used.

Configuration parameter	Meaning
TargetSystem EBS Accounts InitialRandomPassword SendTo MailTemplatePassword	This configuration parameter contains the name of the mail template sent to provide users with information about their initial password. The Employee - initial password for new user account mail template is used.
TargetSystem EBS Accounts MailTemplateDefaultValues	This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account. The Employee - new user account with default properties created mail template is used.
TargetSystem EBS Accounts PrivilegedAccount	This configuration parameter allows configuration of settings for privileged user accounts.
TargetSystem EBS Accounts PrivilegedAccount AccountName_Postfix	This configuration parameter contains the postfix for formatting login names for privileged user accounts.
TargetSystem EBS Accounts PrivilegedAccount AccountName_Prefix	This configuration parameter contains the prefix for formatting login names for privileged user accounts.
TargetSystem EBS DBDeleteOnError	If this configuration parameter is set and a user account cannot be added to the target system, the object is deleted from the database afterward.
TargetSystem EBS DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.
TargetSystem EBS MaxFullsyncDuration	This configuration parameter contains the maximum runtime for synchronization. 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	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem EBS PersonAutoDisabledAccounts	This configuration parameters specifies whether employees are automatically assigned to disable user accounts. User accounts do not obtain an account definition.
TargetSystem EBS	This configuration parameter specifies the mode for

Configuration parameter	Meaning
PersonAutoFullsync	automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem EBS PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names are listed in a pipe () delimited list that is handled as a regular search pattern.

The following configuration parameters are also required.

Table 53: 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	Default email address (sender) for sending notifications.
DPR Journal LifeTime	This configuration parameter specifies the synchronization log's retention period (in days). Use the configuration sub parameters to specify the retention period for each warning level. Older logs are deleted from the database.
QER CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to the parameter require recompiling the database. If the parameter is enabled, values for the risk index can be entered and calculated.
QER Person TemporaryDeactivation	This configuration parameter specifies whether user accounts for an employee are locked if the employee is temporarily or permanently disabled.
QER Person UseCentralPassword	This configuration parameter specifies whether the employee's central password is used in the user accounts. The employee's central password is automatically mapped to the employee's user account in all permitted target systems. This excludes privileged user accounts, which are not updated.

Configuration parameter	Meaning
QER Person UseCentralPassword PermanentStore	This configuration parameter controls the storage period for central passwords. If the configuration parameter is enabled, the central password is stored in the One Identity Manager database and is used for new users. If the configuration parameter is disabled, the central password is deleted from the One Identity Manager database following publishing to the existing user accounts. The central password is not available for new user accounts.
QER Structures Inherite GroupExclusion	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 the parameter require recompiling the database.

Appendix: 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" IsDNColumn="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>
<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" Schema="APPLSYS" APK="" USN="" WhereClause=""
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" Schema="APPLSYS" APK="USER_ID" USN="LAST_UPDATE_
DATE" WhereClause="" 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" Schema="APPLSYS" APK="SECURITY_GROUP_ID"
USN="LAST_UPDATE_DATE" WhereClause="" 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" Schema="APPLSYS" APK="" USN=""
WhereClause="" 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" />
            <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" />
        </Function>
    </Insert>
</Functions>

```

```

        <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 or other inquiries, visit <https://www.oneidentity.com/company/contact-us.aspx> or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

A

- account definition 50
 - add to IT Shop 63
 - assign automatically 62
 - assign to all persons 62
 - assign to business role 61
 - assign to customer 65
 - assign to department 61
 - assign to employee 60, 62
 - assign to location 61
 - assigning to user accounts 72
 - create 51
 - delete 65
 - IT operating data 55, 57
 - manage level 53
- account definitions
 - assign to system roles 63
- application 127
- application role
 - target system managers 146
- APPS user 14
- assign account definition to cost center 61
- attribute 131-132

B

- base object 41

C

- category 115
- configuration parameter 10, 156

- connector schema
 - extend 31
- customer 117, 135
 - account definition (initial) 65

D

- data group 129
- data group unit 129
- default user account 77
- direction of synchronization
 - to Manager 20
 - to target system 20

E

- edit Job server 142
- email notification 92
- employee
 - assign user account 72
 - delete 75
- employee assignment
 - manual 70
 - removing 70
 - search criterion 68
 - user account 73
- entitlement
 - add to IT Shop 99
 - assign business role 97
 - assign category 125
 - assign cost center 96
 - assign department 96

- assign extended property 127
- assign location 96
- assign responsibility 125
- assign role 95
- assign security group 125
- assign system role 98
- assign user account 95, 100
- category 108
- edit assignment 100
- editing 125
- effective 106
- exclude 106
- inheritance via categories 115
- inheritance via roles 95
- inheritance via system roles 98
- overview 127
- overview of all assignments 111
- remove assignment 100
- request via IT Shop request 125
- risk index 125
- entitlement assignment
 - direct 94, 100, 102
 - indirect 94
 - invalid
 - XOrigin 110
- exclusion definition 106
- exclusions attribute 132
- extended property
 - E-Business Suite entitlement 127
 - user account 122

H

- HR employee 133
- HR person 117

I

- identity 75
- inheritance
 - category 108
- initialize system connection 30
- IT operating data
 - change 59
- IT Shop shelf
 - assign account definition 63
 - assign entitlements 99

J

- Job server
 - edit 16
 - properties 143

L

- location 137
- log file 48
- logon information 92

M

- menu 128
 - excluded 132

N

- NLog 48
- notification 92

O

- object
 - delete immediately 45
 - outstanding 45
 - publishing 45
- outstanding object 45

P

- parties 135
- party 117
- password
 - initial 91-92
- password policies
 - editing 85
- password policy 81
 - assign 83
 - character classes 87
 - check password 90
 - default policy 83, 85
 - display name 85
 - error message 85
 - exclusion list 90
 - failed logins 86
 - generate password 91
 - generation script 88-89
 - initial password 86
 - name properties 86
 - password age 86
 - password cycle 86
 - password length 86
 - password strength 86
 - predefined 82
 - test script 88

- permission
 - validity period 104
- personalized admin identity 77
- process group 130
- project template 151

R

- reset revision 48
- reset start information 48
- responsibility 125, 132
 - validity 132
- revision filter 30
- risk assessment
 - entitlement 125
 - user account 117

S

- schedule 42
 - deactivation 44
- schema
 - changes 29
 - compress 29
 - update 29
- schema extension file 31
- schema type
 - create additional 31
 - function definition 39
 - hierarchy 37
 - object definitions 34
 - object key definition 35
 - parameter 40
 - primary key 36
 - table definition 35
 - task definition 38

- variable for language version 41
- security attribute 122, 131-132
- security group 125, 130
- server function 145
- shared identity 77
- single object synchronization 41, 45
- SQL statement 30
- start synchronization 20
- supplier 117, 134
- synchronization
 - basic object
 - create 28
 - configuration 25
 - configure 20
 - connection parameter 25, 28
 - connection parameters 20
 - customize schema 25
 - employee data 23
 - extended schema 28
 - HR data 23
 - only changes 30
 - parties 24
 - permissions 13, 149
 - prerequisite 11
 - prevent 44
 - schedule 42
 - scope 25
 - several E-Business Suite systems 28
 - simulate 48
 - speed up 30
 - start 42
 - suppliers 24
 - synchronization project
 - create 20
 - target system schema 28
 - users 13
 - variable 25
 - variable set 28
 - workflow 20, 27
- synchronization analysis report 48
- synchronization configuration
 - customize 25, 27-28
- synchronization direction
 - to target system 27
- synchronization log 48
 - contents 25
 - create 25
 - display 43
- synchronization project
 - create 20
 - deactivation 44
 - editing 115
 - project template 151
- synchronization server 15
 - configure 15
 - edit 142
 - install 16
 - Job server 16
 - server function 145
 - system requirements 15
- synchronization user 14
- synchronization workflow
 - create 20
 - set up 27
- synchronize single object 45
- system
 - account definition 113
 - application roles 9
 - category 108
 - define categories 115

- edit 113
- employee assignment 68
- reports 137
- synchronization type 113
- target system manager 9, 146

T

- target system manager 146
 - definition 113
- target system reconciliation 45
- template
 - modify IT operating data 59

U

- user account 116
 - administrative user account 77
 - assign employee 67
 - assign entitlement 102
 - assign extended properties 122
 - assigned employee 117
 - assigned permissions 137
 - category 108
 - customer 117
 - data quality 137
 - default user account 77
 - delete 124
 - delete employee 75
 - disable 124
 - disabling 123
 - edit entitlement assignment 102
 - employee assignment 73
 - execute template 59
 - group identity 80
 - HR Person 117

- identity 75
 - linked 72
 - login data 121
 - manage level 71
 - overview 122
 - party 117
 - password 91, 121
 - notification 92
 - personalized admin identity 77
 - privileged user account 75, 78
 - remove entitlement assignment 102
 - risk index 117
 - security attribute 122
 - set up 117
 - shared identity 77
 - status 117
 - supplier 117
 - type 75, 77-78
 - unused 137
 - user entitlement 80
- user for accessing Oracle E-Business Suite 14

V

- validity of a permission assignment 104
- validity period 104

W

- wrapper 14

X

- XOrigin 94