



One Identity Manager 8.2

Administration Guide for Connecting to Oracle E-Business Suite

Copyright 2021 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 highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

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

One Identity Manager Administration Guide for Connecting to Oracle E-Business Suite
Updated - 24 November 2021, 11:02
Version - 8.2

Contents

Mapping an Oracle E-Business Suite in One Identity Manager	9
Architecture overview	9
One Identity Manager users for managing Oracle E-Business Suite	10
Configuration parameters	11
Synchronizing Oracle E-Business Suite	13
Setting up initial synchronization of Oracle E-Business Suite	14
Users and permissions for synchronizing with Oracle E-Business Suite	15
How to prepare the synchronization user	16
Setting up the E-Business Suite synchronization server	17
System requirements for the synchronization server	17
Installing the One Identity Manager Service	18
Creating a synchronization project for initial synchronization of Oracle E-Business Suite	20
Information required for setting up a synchronization project	21
Setting up an initial synchronization project	22
Setting up a synchronization project for employee data	26
Setting up a synchronization project for organizational data	27
Configuring the synchronization log	28
Customizing the synchronization configuration	28
Important notes for adjusting existing synchronization projects	29
Configuring synchronization in Oracle E-Business Suite	30
Configuring synchronization of several Oracle E-Business Suite systems	31
Changing system connection settings of Oracle E-Business Suite systems	32
Editing connection parameters in the variable set	32
Editing target system connection properties	33
Updating schemas	34
Configuring department synchronization	35
Speeding up synchronization with revision filtering	36
Using specific statements for database initialization	36
Using additional schema types	37
Creating a schema extension file	39

Object definitions	40
Table definitions	41
Task definitions	45
Symbolic variables in WHERE clauses	47
Configuring single object synchronization	47
Accelerating provisioning and single object synchronization	48
Running synchronization	49
Starting synchronization	50
Displaying synchronization results	51
Deactivating synchronization	52
Synchronizing single objects	52
Tasks following synchronization	53
Post-processing outstanding objects	53
Adding custom tables to the target system synchronization	55
Troubleshooting	55
Ignoring data error in synchronization	56
Managing E-Business Suite user accounts and employees	58
Setting up account definitions	59
Creating account definitions	60
Main data for account definitions	60
Creating manage levels	62
Main data for manage levels	64
Creating mapping rules for IT operating data	65
Entering IT operating data	66
Modify IT operating data	67
Assigning account definitions to employees	68
Assigning account definitions to departments, cost centers, and locations	69
Assigning account definitions to business roles	69
Assigning account definitions to all employees	70
Assigning account definitions directly to employees	71
Assigning account definitions to system roles	71
Adding account definitions in the IT Shop	71
Assigning account definitions to target systems	74
Deleting account definitions	74
Assigning employees automatically to E-Business Suite user accounts	76

Editing search criteria for automatic employee assignment	78
Finding employees and directly assigning them to user accounts	79
Changing the manage level in user accounts	81
Assigning account definitions to linked user accounts	82
Manually linking employees to E-Business Suite user accounts	82
Linking E-Business Suite user accounts to imported employees	83
Special features for the deletion of employees	84
Supported user account types	85
Default user accounts	86
Administrative user accounts	87
Providing an administrative user account for one employee	88
Providing an administrative user account for multiple employees	89
Privileged user accounts	90
Login information	92
Password policies for E-Business Suite user accounts	92
Predefined password policies	93
Using password policies	94
Editing password policies	95
General main data of password policies	96
Policy settings	96
Character classes for passwords	98
Custom scripts for password requirements	99
Checking passwords with a script	100
Generating passwords with a script	101
Editing the excluded list for passwords	102
Checking passwords	102
Testing the generation of passwords	103
Initial password for new E-Business Suite user accounts	103
Email notifications about login data	104
Managing entitlement assignments	106
Assigning E-Business Suite entitlements to user accounts in One Identity Manager ...	107
Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts	108
Assigning E-Business Suite entitlements to departments, cost centers, and locations	109

Assigning E-Business Suite entitlements to business roles	111
Adding E-Business Suite entitlements to system roles	112
Adding E-Business Suite entitlements to the IT Shop	112
Assigning E-Business Suite user accounts directly to an entitlement	114
Assigning E-Business Suite entitlements directly to a user account	116
Validity period of permission assignments	117
Effectiveness of entitlement assignments	119
Inheritance of E-Business Suite entitlements based on categories	122
Invalid entitlement assignments	124
Overview of all assignments	125
Mapping of E-Business Suite objects in One Identity Manager	127
E-Business Suite systems	127
General main data of E-Business Suite systems	127
Defining categories for the inheritance of E-Business Suite entitlements	129
Editing the synchronization project for a E-Business Suite system	129
E-Business Suite user accounts	130
Entering main data of E-Business Suite user accounts	131
General main data of E-Business Suite user accounts	131
Login data for E-Business Suite user accounts	135
Additional tasks for managing E-Business Suite user accounts	136
Displaying the E-Business Suite user account overview	136
Assigning extended properties to E-Business Suite user accounts	136
Disabling E-Business Suite user accounts	137
Deleting E-Business Suite user accounts	138
E-Business Suite permissions	139
Entering main data of E-Business Suite entitlements	139
General main data of an E-Business Suite entitlement	139
Additional tasks for managing E-Business Suite entitlements	140
Displaying E-Business Suite entitlement overviews	141
Assigning extended properties to E-Business Suite entitlements	141
E-Business Suite applications	142
E-Business Suite menus	142
E-Business Suite data groups	143
E-Business Suite data group units	144
E-Business Suite request groups	144

E-Business Suite security groups	145
E-Business Suite attributes	145
E-Business Suite responsibilities	146
Displaying main data of E-Business Suite responsibilities	147
General main data of E-Business Suite responsibilities	147
HR people	148
Suppliers and contacts	149
Parties	150
Locations	152
Departments	152
Reports about E-Business Suite objects	153
Handling of E-Business Suite objects in the Web Portal	156
Basic configuration data	158
Job server for E-Business Suite-specific process handling	159
Editing E-Business Suite Job servers	159
General main data of Job servers	160
Specifying server functions	162
Target system managers	163
Appendix: Configuration parameters for managing Oracle E-Business Suite	166
Appendix: Permissions required for synchronizing with Oracle E-Business Suite	170
Appendix: Default project templates for synchronizing an Oracle E-Business Suite	173
Project template for user accounts and entitlements	173
Project template for HR data	174
Project template for CRM data	175
Project template for OIM data	175
Appendix: Editing system objects	176
Appendix: Example of a schema extension file	178
About us	182
Contacting us	182
Technical support resources	182

Index183

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.

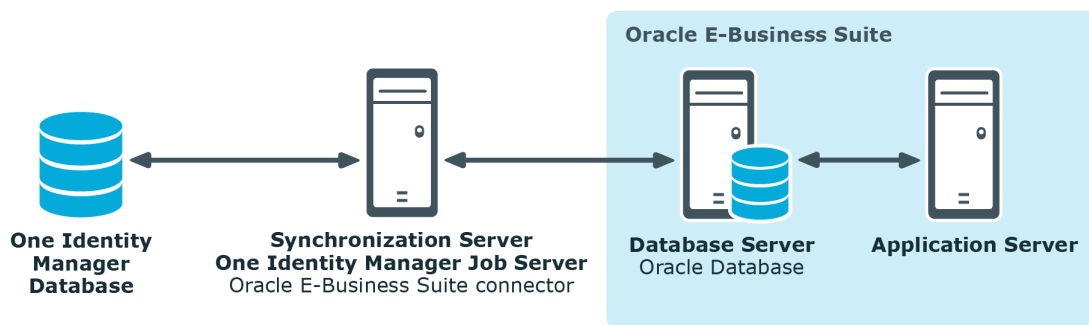
One Identity Manager provides company employees with the user accounts required to allow you to use different mechanisms for connecting employees to their user accounts. You can also manage user accounts independently of employees and therefore set up administrator user accounts.

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 by their E-Business Suite user accounts. Default One Identity Manager functions, such as the IT Shop or Identity Audit, can be used for these people.

Architecture overview

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

Figure 1: Architecture for synchronization



One Identity Manager users for managing Oracle E-Business Suite

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

Table 1: Users

Users	Tasks
Target system administrators	Target system administrators must be assigned to the Target systems Administrators application role. Users with this application role: • Administer application roles for individual target system types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles for target system managers are mutually exclusive. • Authorize other employees to be target system administrators. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the Target systems Oracle E-Business Suite or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects.

Users	Tasks
	• Edit password policies for the target system. • Prepare entitlements to add to the IT Shop. • Can add employees who have another identity than the Primary identity. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	One Identity Manager administrator and administrative system users Administrative system users are not added to application roles. One Identity Manager administrators: • Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required.

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. In the Designer, you can find an overview of all configuration parameters in the **Base data > General > Configuration parameters** category.

For more information, see [Configuration parameters for managing Oracle E-Business Suite](#) on page 166.

Synchronizing Oracle E-Business Suite

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

This section explains how to:

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

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

Detailed information about this topic

- [Setting up initial synchronization of Oracle E-Business Suite](#) on page 14
- [Customizing the synchronization configuration](#) on page 28
- [Running synchronization](#) on page 49
- [Troubleshooting](#) on page 55
- [Editing system objects](#) on page 176

Related topics

- [Architecture overview](#) on page 9

Setting up initial synchronization of Oracle E-Business Suite

The Synchronization Editor provides several project templates with which Oracle E-Business Suite user accounts and entitlements can be selected from either organizational data or data from the Human Resource Module for setting up synchronization. You use these project templates to create synchronization projects with which you import the data from a 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 **TargetSystem | EBS** configuration parameter is set.
 - In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.

NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
 - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
3. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.
4. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- [Users and permissions for synchronizing with Oracle E-Business Suite](#) on page 15
- [System requirements for the synchronization server](#) on page 17
- [Creating a synchronization project for initial synchronization of Oracle E-Business Suite](#) on page 20
- [Configuration parameters for managing Oracle E-Business Suite](#) on page 166
- [Default project templates for synchronizing an Oracle E-Business Suite](#) on page 173

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

User	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 16 and Permissions required for synchronizing with Oracle E-Business Suite on page 170.
One Identity Manager Service user account	The user account for the One Identity Manager Service requires user permissions to carry out operations at file level (adding and editing directories and files). The user account must belong to the Domain users group. The user account must have the Login as a service extended user permissions. The user account requires permissions for the internal web service. NOTE: If the One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can grant permissions for the internal web service with the following command line call: <pre>netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"</pre> The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager. In the default installation, One Identity Manager is installed under: • %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 to run synchronization using an application server.

How to prepare the synchronization user

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

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

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

Scenario 1:

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

Scenario 2:

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

To add the synchronization user

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

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

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

Scenario 3:

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

IMPORTANT: The synchronization user requires:

- All the permissions listed and also
- All **implicit** permissions for the package `apps.fnd_user_pkg`

Detailed information about this topic

- [Permissions required for synchronizing with Oracle E-Business Suite](#) on page 170

Setting up the E-Business Suite synchronization server

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

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

Detailed information about this topic

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

System requirements for the synchronization server

To set up synchronization with Oracle E-Business Suite, a server has to be available that has the following software installed on it:

- Windows operating system
The following versions are supported:
 - Windows Server 2022
 - Windows Server 2019
 - Windows Server 2016
 - Windows Server 2012 R2
 - Windows Server 2012
- 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 declared as a Job server in One Identity Manager.

Table 3: Properties of the Job server

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

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

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

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

NOTE: The program performs a remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program.

To remotely install the One Identity Manager Service, you must have 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*.

NOTE: To generate processes for the Job server, you need the provider, connection parameters, and the authentication data. By default, this information is determined from the database connection data. If the Job server runs through an application server, you must configure extra connection data in the Designer. For detailed information about setting up Job servers, see the *One Identity Manager Configuration Guide*.

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

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

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

- a. Select a Job server from the **Server** menu.

- OR -

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

- b. Enter the following data for the Job server.

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

Syntax:

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

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

4. On the **Machine roles** page, select **E-Business Suite**.
5. On the **Server functions** page, select **Oracle E-Business Suite connector**.
6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

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

- For a direct connection to the database:
 1. Select **Process collection > sqlprovider**.
 2. Click the **Connection parameter** entry, then click the **Edit** button.
 3. Enter the connection data for the One Identity Manager database.
- For a connection to the application server:
 1. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
 2. Click the **Connection parameter** entry, then click the **Edit** button.
 3. Enter the connection data for the application server.
 4. Click the **Authentication data** entry and click the **Edit** button.
 5. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For

detailed information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.
10. If the database is encrypted, on the **Select private key file** page, select the file with the private key.
11. On the **Service access** page, enter the service's installation data.
 - **Computer:** Enter the name or IP address of the server that the service is installed and started on.
 - **Service account:** Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options. You can also change the One Identity Manager Service details, such as the installation directory, name, display name, and the One Identity Manager Service description, using the advanced options.

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 the Server Installer.

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

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

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

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

Information required for setting up a synchronization project

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

Table 4: Information required for setting up a synchronization project

Data	Explanation
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 16.
Data source	TNS alias name from TNSNames.ora. This data is only required if the Oracle E-Business Suite connector can only access the Oracle Database using Oracle Client software.
Synchronization server for Oracle E-Business Suite	All One Identity Manager Service actions are run against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. For more information, see Setting up the E-Business Suite synchronization server on page 17.
One Identity Manager database connection data	• Database server • Database name • SQL Server login and password • Specifies whether integrated Windows authentication is used Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
Remote connection server	To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If direct access is not possible from the workstation, you can set up a remote connection.

Data	Explanation
	The remote connection server and the workstation must be in the same Active Directory domain. Remote connection server configuration: • One Identity Manager Service is started • RemoteConnectPlugin is installed • Oracle E-Business Suite connector is installed The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required. For more detailed information about setting up a remote connection, see the <i>One Identity Manager Target System Synchronization Reference Guide</i>.

Setting up an initial synchronization project

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

- Run in default mode
- Started from the Launchpad

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

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

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

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

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

1. Start the Launchpad and log in on the One Identity Manager database.
NOTE: If synchronization is run by an application server, connect the database through the application server.
2. Select the **Target system type Oracle E-Business Suite** entry and click **Start**.
This starts the Synchronization Editor's project wizard.
3. On the **System access** page, specify how One Identity Manager can access the target system.
 - If access is possible from the workstation on which you started the Synchronization Editor, do not change any settings.
 - If access is not possible from the workstation on which you started the Synchronization Editor, you can set up a remote connection.
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 5: 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. Deactivate this option to access using Oracle Client software. Which connection data is required, depends on how this option is set.
Server	Name of the server on which the Oracle Database is installed. The fully qualified server name or the IP address may be given. The server ID is used to format the E-Business Suite system display name in the One Identity Manager database.
Port	Port of the Oracle instance.
Service name	Name of the service.
User	User name used by the connector to log in to the Oracle Database.
Password	Password for logging in to the Oracle Database.
Data sources	TNS alias name from TNSNames.ora.

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

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

Table 6: Connection configuration

Property	Description
Language selection	Languages used to load captions from the database.
Unique name for the DN.	Part of name used to generate a distinguished name for all objects in the system. Leave this field empty to use the database server's server name. This name should not be changed after the initial synchronization.
Read-only	Specifies whether the Oracle E-Business Suite connector only has read access to the target system.
Package to access users	The name of the wrapper package or user package to be used for adding and modifying user accounts and permissions. Syntax: <owner>.<PackageName> The following input required, depending on which scenario was used to set up the synchronization user. • 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. On the **Display Name** page, enter a unique display name for the connection configuration.

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

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

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.

- d. **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**.

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

NOTE:

- If enabled, a consistency check is carried out. If errors occur, a message appears. You can decide whether the synchronization project can remain activated or not.

Check the errors before you use the synchronization project. To do this, in the **General** view on the Synchronization Editor's start page, click **Verify project**.

- If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project**

automatically option. In this case, save the synchronization project manually before closing the Synchronization Editor.

Related topics

- [Configuring the synchronization log](#) on page 28
- [Customizing the synchronization configuration](#) on page 28
- [Project template for user accounts and entitlements](#) on page 173
- [Setting up a synchronization project for employee data](#) on page 26
- [Setting up a synchronization project for organizational data](#) on page 27

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.

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

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

To set up a synchronization project for 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 22
- [Project template for HR data](#) on page 174

Related topics

- [Configuring department synchronization](#) on page 35

Setting up a synchronization project for organizational data

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

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

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

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

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

To set up a synchronization project for supplier contact data

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

To set up a synchronization project for party 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 22
- [Project template for CRM data](#) on page 175
- [Project template for OIM data](#) on page 175

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 **Configuration > Target system** category in the Synchronization Editor.
- OR -
To configure the synchronization log for the database connection, select the **Configuration > One Identity Manager connection** category in the 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 analyzes.
5. Click **OK**.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Related topics

- [Displaying synchronization results](#) on page 51

Customizing the synchronization configuration

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

You must customize the synchronization configuration in order to compare the database with the Oracle E-Business Suite regularly and to synchronize changes.

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

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

Detailed information about this topic

- [Configuring synchronization in Oracle E-Business Suite](#) on page 30
- [Configuring synchronization of several Oracle E-Business Suite systems](#) on page 31
- [Updating schemas](#) on page 34
- [Using specific statements for database initialization](#) on page 36
- [Using additional schema types](#) on page 37
- [Changing system connection settings of Oracle E-Business Suite systems](#) on page 32

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 changed by the system connection wizard.

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

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

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

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

Configuring synchronization in Oracle E-Business Suite

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

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

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

1. In the Synchronization Editor, open the synchronization project.
2. Check whether the existing mappings can be used to synchronize into the target system. Create new maps if required.

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

Related topics

- [Configuring synchronization of several Oracle E-Business Suite systems](#) on page 31

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

To customize a synchronization project for synchronizing another system

1. Supply a user in the other system with sufficient permissions for accessing the Oracle E-Business Suite.
2. In the Synchronization Editor, open the synchronization project.
3. Create a new base object for the other system.
 - Use the wizard to attach a base object.
 - In the wizard, select the Oracle E-Business Suite connector.
 - Declare the connection parameters. The connection parameters are saved in a special variable set.

A start up configuration is created that uses the newly created variable set.

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

Related topics

- [Configuring synchronization in Oracle E-Business Suite](#) on page 30

Changing system connection settings of Oracle E-Business Suite systems

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

- a. Specify a specialized variable set and change the values of the affected variables.
The default values remain untouched in the default variable set. The variables can be reset to the default values at any time. (Recommended action).
- b. Edit the target system connection with the system connection wizard and change the effected values.
The system connection wizard supplies additional explanations of the settings. The default values can only be restored under particular conditions.

Detailed information about this topic

- [Editing connection parameters in the variable set](#) on page 32
- [Editing target system connection properties](#) on page 33

Editing connection parameters in the variable set

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

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

To customize connection parameters in a specialized variable set

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
3. Open the **Connection parameters** view.
Some connection parameters can be converted to variables here. For other parameters, variables are already created.
4. Select a parameter and click **Convert**.

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

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

Related topics

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

Editing target system connection properties

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

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

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

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

To edit connection parameters using the system connection wizard

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

NOTE: If the default variable set is selected, the default values are overwritten and cannot be restored at a later time.
3. Select the **Configuration > Target system** category.
4. Click **Edit connection**.
This starts the system connection wizard.
5. Follow the system connection wizard instructions and change the relevant properties.
6. Save the changes.

Related topics

- [Editing connection parameters in the variable set](#) on page 32

Updating schemas

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

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

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

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

To update a system connection schema

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
 - OR -
 - Select the **Configuration > One Identity Manager connection** category.
3. Select the **General** view and click **Update schema**.
4. Confirm the security prompt with **Yes**.

This reloads the schema data.

To edit a mapping

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

Opens the Mapping Editor. For more information about mappings, see the *One Identity Manager Target System Synchronization Reference Guide*.

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

Configuring department synchronization

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

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

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

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

Related topics

- [Setting up a synchronization project for employee data](#) on page 26

Speeding up synchronization with revision filtering

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

Oracle E-Business Suite supports revision filtering. The E-Business Suite objects' date of last change is used as a revision counter. Each synchronization saves the last date is was run as a revision in the One Identity Manager database (DPRRevisionStore table, Value column). This value is used as a comparison for revision filtering when the same workflow is synchronized the next time. When this workflow is synchronized the next time, the 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 modified by synchronization are loaded and checked by the next synchronization. This means that the second synchronization after initial synchronization is not significantly faster.

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

To permit revision filtering on a workflow

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

To permit revision filtering for a start up configuration

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

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

Using specific statements for database initialization

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

To use additional statements for database initialization:

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

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

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

Example of a multi-line statement

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

- d. Click **Test**.
- e. End the system connection wizard.

This updates the connection parameters.

4. Save the changes.

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

Using additional schema types

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

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

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

Check the schema type list before you enable the synchronization project.

To start the Target System Browser

1. Open the synchronization project in the Synchronization Editor.
2. Select **Configuration | Target system**.
3. Select the **General** view and click **Browse**.

This opens the Target System Browser. You will see all the schema types used in this synchronization project in the upper pane of the **Schema types** view. The lower pane contains the list of unused schema types

To extend the connector schema with your own schema types

1. Find which out schema types you require.
2. Create a schema extension file. Save this file and keep the file name and path at the ready.

For more information, see [Creating a schema extension file](#) on page 39.

3. Open the synchronization project in the Synchronization Editor.
4. Enable expert mode.
5. Select the **Configuration > Target system** category.
6. Click **Edit connection**.

This starts the system connection wizard.

7. Verify the data.
8. Enter the path to the schema extension file on the **Schema extensions (manually)** page.
 - a. To check the schema extensions file for logical errors, click **Test file**.
All defined schema types are listed.
 - b. Click **Next**.

9. Click **Finish** to end the system connection wizard.
10. Select the view **General** and click **Update schema**.
11. Confirm the security prompt with **Yes**.

The schema types, including your new schema types, are loaded.

12. Open the Target System Browser and check whether the schema types have been added.

The schema types are displayed in the list of used schema types.

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

15. Save the changes.
16. Run a consistency check.
17. Activate the synchronization project.

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

1. Delete all mappings and synchronization steps that were created for the additional schema types.
2. Edit the target system connection using the system connection wizard.
 - On the **Expert schema settings** page, click **Clear existing**.
3. Update the schema.
4. Save the changes.
5. Run a consistency check.
6. Activate the synchronization project.

Creating a schema extension file

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

You can only specify one schema extension file. This must 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>
```

```
</Object>
</ObjectNames>
</EBSF12>
```

Detailed information about this topic

- [Object definitions](#) on page 40
- [Table definitions](#) on page 41
- [Task definitions](#) on page 45
- [Example of a schema extension file](#) on page 178

Object definitions

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

Example: AK.AK_ATTRIBUTES_TL.ATTRIBUTE_CODE

Table 7: Attributes of an object definition

Attribute	Description
SchemaName	Freely selected name of the schema type to be defined. The objects of this type are displayed in the extended schema under this name.
ParentSchemaName	Reference to an additional schema type on a higher hierarchy level. Example: Application is ParentSchemaName of Attribute
DisplayPattern	Definition of a display pattern for displaying objects in the Synchronization Editor (for example, in the target system browser or when defining schema classes).
IsReadOnly	Specifies whether the objects of this schema type can be read-only. The default value is 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 8: Attributes of an object key definition

Attribute	Description
Column	Name of the column in full name notation.
IsReferencedColumn	Specifies whether the key column is required by other schema types for reference resolution The default value is 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 9: Attributes of a table definition

Attribute	Description
Name	Name of the table (without schema name).
Schema	Name of the Oracle schema.
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.
JoinParentTable	Name of a parent table when a join operation is carried out on a schema type higher up in the hierarchy.
JoinParentColumn	Comma-delimited list of columns in a parent table when a Join operation is carried out on a schema type higher up in the hierarchy (full notation).
JoinChildColumn	Comma-delimited list of columns in the currently defined table to be joined to the columns from JoinParentColumn in the Join operation (full notation). The sequence of columns in the list determines which columns are joined to each other.
View	Name of the view if there is a view for the table that filters the table contents based on the current database edition. Example: Specify the FND_RESPONSIBILITY_TL# view for the FND_RESPONSIBILITY_TL table.

Example

<Tables>

...

```

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

```

...

</Tables>

Primary key definition

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

Table 10: Attribute of a primary key definition

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

Example

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

Column pairs in the hierarchy

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

Table 11: Attributes of a column pair

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

Example

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

Example of a complete table definition

```
<Object SchemaName="ORA-Responsibility" ParentSchemaName="ORA-Application"
DisplayPattern="%vrtDistinguishedName%" IsReadOnly="true" UseDistinct="false">
  <ObjectKey>
    <Key Column="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID"
      IsDNColumn="true" IsReferencedColumn="true" X500Abbreviation="RE" />
    <Key Column="APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID" />
  </ObjectKey>
</Tables>
```

```

<Table Name="FND_RESPONSIBILITY" View="FND_RESPONSIBILITY#"
Schema="APPLSYS" APK="" USN="" WhereClause="" JoinParentTable=""
JoinParentColumn="" JoinChildColumn="" >

    <PK Column="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID" />

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

</Table>

<Table Name="FND_RESPONSIBILITY_TL" View="FND_RESPONSIBILITY_TL#"
Schema="APPLSYS" APK="" USN="APPLSYS.FND_RESPONSIBILITY_TL.LAST_UPDATE_
DATE" WhereClause="APPLSYS.FND_RESPONSIBILITY_TL.LANGUAGE='$SYSLANGU$'"
JoinParentColumn="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID,APPLSYS.FND_
RESPONSIBILITY.APPLICATION_ID" JoinParentTable="FND_RESPONSIBILITY"
JoinChildColumn="APPLSYS.FND_APPLICATION.APPLICATION_ID" >

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

</Table>

<Table Name="FND_APPLICATION" View="FND_APPLICATION#" Schema="APPLSYS"
APK="" USN="" WhereClause="" JoinParentTable="FND_RESPONSIBILITY"
JoinParentColumn="APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID"
JoinChildColumn="APPLSYS.FND_APPLICATION.APPLICATION_ID" >

    <PK Column="APPLSYS.FND_APPLICATION.APPLICATION_ID" />

</Table>

</Tables>

</Object>

```

Explanation

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

The schema type is subordinate to the ORA-Application schema type in the hierarchy (ParentSchemaName). It has two object key columns (APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID and APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID), of which only one is included as a part of the distinguished name `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 47.

Task definitions

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

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

Structure of the task definitions

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

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

Function definitions

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

Table 12: Attributes of a function definition

Attribute	Description
Name	Name of the function. Full notation in the form <Schema name>.<Package name>.<Function name>.
OrderNumber	Numerical specification of the run sequence. The default value is 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 running the functions of this package, you may need to implement a wrapper package that changes the call context. The name of this wrapper package can be saved in the connection configuration. It is replaced at runtime before running the function in the SQL block. The symbolic variable for the defined package name is \$ebsUserPackageName\$. For more information, see [Setting up an initial synchronization project](#) on page 22.

Example

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

Parameter definitions

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

Table 13: Attributes of a parameter definition

Attribute	Description
Name	Name of the parameter in the function definition.
PropertyName	Name of the object property whose value is to be transferred (full notation). - OR - Fixed value, if PropertyType="FIX" is defined.
PropertyType	Data type Possible values: • 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. In three cases, a null value definition makes sense:

Attribute	Description
	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 the 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 running 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 the object is no longer present in the target system, then it is deleted from the One Identity Manager database.

Prerequisites

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

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

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

1. In the Manager, select the **Oracle E-Business Suite > Basic configuration data > Target system types** category.
2. In the result list, select the **Oracle E-Business Suite** target system type.
3. Select the **Assign synchronization tables** task.
4. In the **Add assignments** pane, assign the custom table for which you want to use single object synchronization.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the custom table and enter the **Root object path**.
Enter the path to the base object in the ObjectWalker notation of the VI.DB.
Example: FK(UID_EBSSystem).XObjectKey
8. Save the changes.

Related topics

- [Synchronizing single objects](#) on page 52
- [Post-processing outstanding objects](#) on page 53

Accelerating provisioning and single object synchronization

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

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

have not been completely processed.

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

To configure load balancing

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

All Job servers must access the same E-Business Suite as the synchronization server for the respective base object.

2. In the Synchronization Editor, assign a custom server function to the base object.

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

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

For more information about editing base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.

3. In the Manager, assign this server function to all the Job servers that will be processing provisioning and single object synchronization for the base object.

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

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

To use the synchronization server without load balancing.

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

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

Detailed information about this topic

- [Editing E-Business Suite Job servers](#) on page 159

Running synchronization

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

If you want to specify the order in which target systems are synchronized, use the start up sequence to run synchronization. In a start up sequence, you can combine start up configurations from different synchronization projects and specify the order in which they are run. For more information about start up sequences, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- [Starting synchronization](#) on page 50
- [Deactivating synchronization](#) on page 52
- [Displaying synchronization results](#) on page 51

Starting synchronization

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

To synchronize on a regular basis

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

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

To start initial synchronization manually

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

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

- If another synchronization process is started with the same start up configuration, the process is stopped and is assigned **Frozen** status. An error message is written to the One Identity Manager Service log file.

- Ensure that start up configurations that are used in start up sequences are not started individually at the same time. Assign start up sequences and start up configurations different schedules.
- Starting another synchronization process with different start up configuration that addresses same target system may lead to synchronization errors or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration.
 - Use the schedule to ensure that the start up configurations are run in sequence.
 - Group start up configurations with the same start up behavior.

Displaying synchronization results

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

To display a synchronization log

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

To display a provisioning log

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

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

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

Related topics

- [Configuring the synchronization log](#) on page 28
- [Troubleshooting](#) on page 55

Deactivating synchronization

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

To prevent regular synchronization

1. In the Synchronization Editor, open the synchronization project.
2. Select the start up configuration and deactivate the configured schedule.

Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

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

Synchronizing single objects

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

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

To synchronize a single object

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

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

Detailed information about this topic

- [Configuring single object synchronization](#) on page 47

Tasks following synchronization

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

- [Post-processing outstanding objects](#) on page 53

Post-processing outstanding objects

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

Outstanding objects:

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

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

Start target system synchronization to do this.

To post-process outstanding objects

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

The navigation view lists all the synchronization tables assigned to the **Oracle E-Business Suite** target system type.

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

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

- The synchronization log has already been deleted.
- OR -
- An assignment from a member list has been deleted from the target system.

The base object of the assignment was updated during the synchronization. A corresponding entry appears in the synchronization log. The entry in the assignment table is marked as outstanding, but there is no entry in the synchronization log.

- An object that contains a member list has been deleted from the target system.

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

TIP:

To display object properties of an outstanding object

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

Table 14: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account. The Outstanding label is removed from the object. Indirect memberships cannot be deleted.
	Publish	The object is added to the target system. The Outstanding label is removed from the object. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: • The table containing the object can be published. • The target system connector has write access to the target system.
	Reset	The Outstanding label is removed for the object.

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

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

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

To disable bulk processing

- Disable the  icon in the form's toolbar.

NOTE: The target system connector must have write access to the target system in order to publish outstanding objects that are being post-processed. That means, the **Connection is read-only** option must not be set for the target system connection.

Adding custom tables to the target system synchronization

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

To add tables to target system synchronization

1. In the Manager, select the **Oracle E-Business Suite > Basic configuration data > Target system types** category.
2. In the result list, select the **Oracle E-Business Suite** target system type.
3. Select the **Assign synchronization tables** task.
4. In the Add assignments pane, assign **custom** tables to the outstanding objects you want to handle.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the custom tables that contain the outstanding objects that can be published in the target system and set the **Publishable** option.
8. Save the changes.

Related topics

- [Post-processing outstanding objects](#) on page 53

Troubleshooting

Synchronization Editor helps you to analyze and eliminate synchronization errors.

- **Simulating synchronization**
The simulation allows you to estimate the result of synchronization. This means you can, for example, recognize potential errors in the synchronization configuration.
- **Analyzing synchronization**
You can generate the synchronization analysis report for analyzing problems which occur during synchronization, for example, insufficient performance.

- Logging messages

One Identity Manager offers different options for logging errors. These include the synchronization log, the log file for One Identity Manager Service, the logging of messages with NLOG, and similar.

- Reset start information

If synchronization stopped unexpectedly, for example, because a server was not available, the start information must be reset manually. Only then can the synchronization be restarted.

- Resetting revisions

It may also be necessary to process those objects during synchronization, whose change information has not been updated since the last synchronization. This might be required if changes to data were made without the change information for the object being updated, for example. This means, the change information for objects becomes older than that saved in the synchronization project. In such cases, the revision for a start up configuration can be reset.

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

Related topics

- [Displaying synchronization results](#) on page 51

Ignoring data error in synchronization

By default, objects with incorrect data are not synchronized. These objects can be synchronized once the data has been corrected. In certain situations, however, it might be necessary to synchronize objects like these and ignore the data properties that have errors. This synchronization behavior can be configured in One Identity Manager.

To ignoring data errors during synchronization in One Identity Manager

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

This starts the system connection wizard.

4. On the **Additional options** page, enable **Try to ignore data errors**.

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

Default columns, such as primary keys, UID columns, or mandatory input columns cannot be ignored.

5. Save the changes.

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

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

Managing E-Business Suite user accounts and employees

The main feature of One Identity Manager is to map employees together with the main data and permissions available to them in different target systems. To achieve this, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to employees. This provides an overview of the permissions for each employee in all of the connected target systems. One Identity Manager offers the option of managing user accounts and their permissions. You can provision modifications in the target systems. 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 methods 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 is not the One Identity Manager default method. You must 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 through automatic employee assignment, account definitions, or manually.

For more 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 59
- [Assigning employees automatically to E-Business Suite user accounts](#) on page 76
- [Entering main data of E-Business Suite user accounts](#) on page 131
- [Linking E-Business Suite user accounts to imported employees](#) on page 83

Setting up account definitions

One Identity Manager has account definitions for automatically allocating user accounts to employees. 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 central 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. Processing is done through templates. There are predefined templates for determining the data required for user accounts included in the default installation. You can customize templates as required.

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

The following steps are required to implement an account definition:

- [Creating 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 or edit an account definition

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

Main data for account definitions

Enter the following data for an account definition:

Table 15: Main data for an account definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema that maps user accounts.
Target system	Target system to which the account definition applies.
Required account definition	Specifies the required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is assigned automatically. Leave empty for E-Business Suite systems.
Description	Text field for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	Value for evaluating the risk of assigning the account definition to employees. Set a value in the range 0 to 1. This input field is only visible if the QER CalculateRiskIndex configuration parameter is set. For detailed information, see the <i>One Identity Manager Risk Assessment Administration Guide</i>.
Service item	Service item through which you can request the account definition resource in the IT Shop. Assign an existing service

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

Property	Description
	Option not set (default): The account definition assignment is not in effect. The associated user account is disabled.
Retain account definition on security risk	Specifies the account definition assignment to employees posing a security risk. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is disabled.
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.
Entitlements can be inherited	Specifies whether the user account can inherit E-Business Suite permissions through the employee. If this option is set, the user account inherits permissions through hierarchical roles or IT Shop requests. 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 E-Business Suite entitlement in the IT Shop. The request is approved and assigned. The user account only inherits this entitlement if this option is active.

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** manage levels are analyzed in templates. You can customize the supplied templates in the Designer.

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

Specify 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.

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

To assign manage levels to an account definition

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

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

To remove an assignment

- Select the manage level and double-click .
5. Save the changes.

To edit a manage level

1. In the Manager, select the **Oracle E-Business Suite > Basic configuration data > Account definitions > Manage levels** category.
2. Select the manage level in the result list. Select the **Change main data** task.
– OR –
Click  in the result list.
3. Edit the manage level's main data.
4. Save the changes.

Main data for manage levels

Enter the following data for a manage level.

Table 16: Main data for manage levels

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

Property	Description
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 disabled user accounts retain their group memberships.

Related topics

- [Invalid entitlement assignments](#) on page 124

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 automatically creating user accounts for an employee in the target system and modifying them.

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

To create a mapping rule for IT operating data

1. In the Manager, select the **Oracle E-Business Suite > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Edit IT operating data mapping** task.
4. Click **Add** and enter the following information:
 - **Column:** User account property for which the value is set. In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.
 - **Source:** Specifies which roles to use in order to find the user account properties. You have the following options:
 - Primary department
 - Primary location
 - Primary cost center
 - Primary business roles

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

- Empty

If you select a role, you must specify a default value and set the **Always use default value** option.

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

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

5. Save the changes.

Entering IT operating data

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

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

Example:

In the IT operating data mapping rule for the account definitions A and B, specify the **Department** property in order to determine the valid IT operating data.

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

To define IT operating data

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

3. Click **Add** and enter the following data.

- **Effects on:** Specify an IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.

To specify an application scope

- a. Click ➔ next to the field.
- b. Under **Table**, select the table that maps the target system for select the TSBAccountDef table or an account definition.
- c. Select the specific target system or account definition under **Effects on**.
- d. Click **OK**.

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

In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.

- **Value:** Enter a fixed value to assign to the user account's property.

4. Save the changes.

Modify IT operating data

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

Prerequisites

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

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

To run the template

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

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

- **Old value:** Value of the object property before changing the IT operating data.
 - **New value:** Value of the object property after changing the IT operating data.
 - **Selection:** Specifies whether the new value is copied to the user account.
4. Mark all the object properties in the **selection** column that will be given the new value.
 5. Click **Apply**.

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

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

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

NOTE: If a user account already exists and is disabled, then it is re-enabled. In this case, you must change the user account manage level afterward.

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 account definition assignment is removed, the user account that was created from this account definition is disabled.

Prerequisites for indirect assignment of account definitions to employees

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

To configure assignments to roles of a role class

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

For 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 the **Oracle E-Business Suite > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
 - On the **Departments** tab, assign departments.
 - On the **Locations** tab, assign locations.
 - On the **Cost centers** tab, assign cost centers.

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

To remove an assignment

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

Assigning account definitions to business roles

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

To add account definitions to hierarchical roles

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

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

To remove an assignment

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

Assigning account definitions to all employees

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

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

To assign an account definition to all employees

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

NOTE: To automatically remove the account definition assignment from all employees, run the **DISABLE AUTOMATIC ASSIGNMENT TO EMPLOYEES** task. 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 the **Oracle E-Business Suite > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign to employees** task.
4. In the **Add assignments** pane, add employees.

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

To remove an assignment

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

Assigning account definitions to system roles

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

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

To add account definitions to a system role

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

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

To remove an assignment

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

Adding account definitions in the IT Shop

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

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

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

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

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

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

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. Save the changes.

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

1. In the Manager, select the **Oracle E-Business Suite > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. Save the changes.

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

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.
5. Save the changes.

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

1. In the Manager, select the **Oracle E-Business Suite > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.
5. Save the changes.

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

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

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

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

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

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

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

Related topics

- [Main data for account definitions](#) on page 60

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 (**Linked configured** state):

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

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

To assign the account definition to a target system

1. In the Manager, select the system in the **Oracle E-Business Suite > Systems** category.
2. Select the **Change main data** task.
3. From the **Account definition (initial)** menu, select the account definition for user accounts.
4. Save the changes.

Detailed information about this topic

- [Assigning employees automatically to E-Business Suite user accounts](#) on page 76

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 the **Oracle E-Business Suite > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Change main data** task.
 - d. Select the **Disable automatic assignment to employees** task.
 - e. Confirm the security prompt with **Yes**.
 - f. Save the changes.
2. Remove direct assignments of the account definition to employees.

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

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

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

- a. In the Manager, select the **Entitlements > Account definitions** category.
- b. Select an account definition in the result list.
- c. Select the **Remove from all shelves (IT Shop)** task.
- d. Confirm the security prompt with **Yes**.
- e. Click **OK**.

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

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

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

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.
6. Remove the required account definition assignment. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.
 - a. In the Manager, select the **Oracle E-Business Suite > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Change main data** task.
 - d. From the **Required account definition** menu, remove the account definition.
 - e. Save the changes.
 7. Remove the account definition's assignments to target systems.
 - a. In the Manager, select the system in the **Oracle E-Business Suite > Systems** category.
 - b. Select the **Change main data** task.
 - c. On the **General** tab, remove the assigned account definitions.
 - d. Save the changes.
 8. Delete the account definition.
 - a. In the Manager, select the **Oracle E-Business Suite > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Click  to delete an account definition.

Assigning employees automatically to E-Business Suite user accounts

When you add a user account, an existing employee can automatically be assigned to it. This mechanism can be triggered after a new user account is created either manually or

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

Define criteria for finding employees to apply to automatic employee assignment. If a user account is linked to an employee through the current mode, the user account is given, through an internal process, the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

If you run this procedure during working hours, automatic assignment of employees to user accounts takes place from that moment onwards. If you disable the procedure again later, the changes only affect user accounts added or updated after this point in time. Existing employee assignments 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 main data** to assign employees to administrative user accounts for the respective user account.

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

Run the following tasks to assign employees automatically.

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

Example:

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

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

To edit the exclude list for automatic employee assignment

1. In the Designer, edit the **PersonExcludeList** configuration parameter.
2. Click ... next to the **Value** field.
This opens the **Exclude list for automatic employee assignment** dialog.
3. To add a new entry, click  **Add**.
To edit an entry, select it and click  **Edit**.
4. Enter the name of the user account that does not allow employees to be assigned automatically.

Each entry in the list is handled as part of a regular expression. You are allowed to use the usual special characters for regular expressions.

5. To delete an entry, select it and click  **Delete**.

6. Click **OK**.

- Use the **TargetSystem | EBS | PersonAutoDisabledAccounts** configuration parameter to specify whether 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.

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.

Related topics

- [Creating account definitions](#) on page 60
- [Assigning account definitions to target systems](#) on page 74
- [Changing the manage level in user accounts](#) on page 81
- [Editing search criteria for automatic employee assignment](#) on page 78

Editing search criteria for automatic employee assignment

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.

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

To specify criteria for employee assignment

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

Table 17: 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)
	Employee (UID_Person)	HR employee (UID_PersonEmployee)

5. Save the changes.

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

Related topics

- [Assigning employees automatically to E-Business Suite user accounts](#) on page 76
- [Finding employees and directly assigning them to user accounts](#) on page 79

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 18: 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

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

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

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

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

To assign employees directly over a suggestion list

- Click **Suggested assignments**.
 1. Click the **Selection** box of 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 the **Selection** box of 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 the **Selection** box of all the user accounts you want to delete the employee assignment from. 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 the Manager, select the **Oracle E-Business Suite > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Select the manage level in the **Manage level** list on the **General** tab.
5. Save the changes.

Related topics

- [General main data of E-Business Suite user accounts](#) on page 131

Assigning account definitions to linked user accounts

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

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

To select user accounts through account definitions

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

Detailed information about this topic

- [Assigning account definitions to target systems](#) on page 74

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.

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

Related topics

- [Supported user account types](#) on page 85

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 (ImportSource column). 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. In the Manager, select the **Oracle E-Business Suite > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Select the **General** tab.
5. Select the HR person from the **HR person** 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 by the EBSUser.UID_Person column.

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

Table 19: 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

Property	Description
	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='EBSCRM').

Detailed information about this topic

- [Managing E-Business Suite user accounts and employees](#) on page 58
- [Editing search criteria for automatic employee assignment](#) on page 78

Related topics

- [Setting up a synchronization project for employee data](#) on page 26
- [Setting up a synchronization project for organizational data](#) on page 27
- [HR people](#) on page 148
- [Parties](#) on page 150
- [Suppliers and contacts](#) on page 149

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 **INACTIVE** status.

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 138
- [Disabling E-Business Suite user accounts](#) on page 137

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 20: 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
Personalized admin identity	User account with administrative permissions, used by one employee.	Admin
Sponsored identity	User account used for a specific purpose. For example, for training purposes.	Sponsored
Shared identity	User account with administrative permissions, used by 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 personalized admin identity are used for different user accounts, which can be used by the same actual employee to perform their different tasks within the company.

To provide user accounts with a personalized 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 permissions to the different user accounts.

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

For more 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 labeled with the **Privileged user account** property (IsPrivilegedAccount column).

Detailed information about this topic

- [Default user accounts](#) on page 86
- [Administrative user accounts](#) on page 87
- [Privileged user accounts](#) on page 90

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 IT operating data for user accounts and which default values are used if no IT operating data can be determined through a person's primary roles.

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

- In the mapping rule for the IsGroupAccount column, use the default value **1** and enable the **Always use default value** option.
- In the mapping rule for the IdentityType column, use the default value **Primary** and enable **Always use default value**.

4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.

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

5. Assign the account definition to 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 59

Administrative user accounts

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

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

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

You can label administrative user accounts as a **Personalized administrator identity** or as a **Shared identity**. Proceed as follows to provide the 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 pseudo employee using the UID_Person column.
Use an employee with the same identity or create a new employee.
3. Assign this pseudo employee to hierarchical roles.

The pseudo employee provides the user account with its permissions.

Related topics

- [Providing an administrative user account for one employee](#) on page 88
- [Providing an administrative user account for multiple employees](#) on page 89

Providing an administrative user account for one employee

Prerequisites

- The user account must be labeled as a personalized admin identity.
- The employee who will be using the user account must be labeled as a personalized admin identity.
- The employee who will be using the user account must be linked to a main identity.

To prepare an administrative user account for a person

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

TIP: If you are the target system manager, you can choose  to create a new person.

Related topics

- [Providing an administrative user account for multiple employees](#) on page 89
- For more information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Providing an administrative user account for multiple employees

Prerequisite

- The user account must be labeled as a shared identity.
- A pseudo employee must exist. The pseudo employee must be labeled as a shared identity and must have a manager.
- The employees who are permitted to use the user account must be labeled as a primary identity.

To prepare an administrative user account for multiple employees

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

TIP: If you are the target system manager, you can choose  to create a new pseudo employee.
3. Assign the employees who will use this administrative user account to the user account.
 - a. In the Manager, select the **Oracle E-Business Suite > User accounts** category.
 - b. Select the user account in the result list.
 - c. Select the **Assign employees authorized to use** task.
 - d. In the **Add assignments** pane, add employees.

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

To remove an assignment

- Select the employee and double-click .

Related topics

- [Providing an administrative user account for one employee](#) on page 88
- For more information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

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 labeled with the **Privileged user account** property (IsPrivilegedAccount column).

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

To create privileged users through account definitions

1. Create an account definition. Create a new manage level for privileged user accounts and assign this manage level to the account definition.
2. If you want to prevent the properties for privileged user accounts from being overwritten, set the **IT operating data overwrites** property for the manage level to **Only initially**. In this case, the properties are populated just once when the user accounts are created.
3. Specify 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 the IT operating data.

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

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

- In the mapping rule for the IsPrivilegedAccount column, use the default value **1** and set the **Always use default value** option.

- You can also specify a mapping rule for the IdentityType column. The column owns different permitted values that represent user accounts.
 - To prevent privileged user accounts from inheriting the entitlements of the default user, define a mapping rule for the IsGroupAccount column with a default value of **0** and set the **Always use default value** option.
5. Enter the effective IT operating data for the target system.
Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.
 6. Assign the account definition directly to 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, specify how the login names are formatted in the template.

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

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

Related topics

- [Setting up account definitions](#) on page 59

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 92
- [Initial password for new E-Business Suite user accounts](#) on page 103
- [Email notifications about login data](#) on page 104

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 93
- [Using password policies](#) on page 94
- [Editing password policies](#) on page 95
- [Custom scripts for password requirements](#) on page 99
- [Editing the excluded list for passwords](#) on page 102

- [Checking passwords](#) on page 102
- [Testing the generation of passwords](#) on page 103

Predefined password policies

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

Password for logging in to One Identity Manager

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

NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for 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** 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** does not violate the target 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** default policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

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

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

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

Using password policies

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

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

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

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

1. Password policy of the user account's account definition.
2. Password policy of the user account's manage level.
3. Password policy of the user account's E-Business Suite system.
4. The **One Identity Manager password policy** (default policy).

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

To reassign a password policy

1. In the Manager, select the **Oracle E-Business Suite > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Click **Add** in the **Assignments** section and enter the following data.
 - **Apply to:** Application scope of the password policy.

To specify an application scope

1. Click ➔ next to the field.
2. Select one of the following references under **Table**:
 - The table that contains the base objects of synchronization.
 - To apply the password policy based on the account definition, select the **TSBAccountDef** table.

- To apply the password policy based on the manage level, select the **TSBBehavior** table.
3. Under **Apply to**, select the table that contains the base objects.
 - If you have selected the table containing the base objects of synchronization, next select the specific target system.
 - If you have selected the **TSBAccountDef** table, next select the specific account definition.
 - If you have selected the **TSBBehavior** table, next select the specific manage level.
 4. Click **OK**.
 - **Password column**: Name of the password column.
 - **Password policy**: Name of the password policy to use.
 5. Save the changes.

To change a password policy's assignment

1. In the Manager, select the **Oracle E-Business Suite > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select the **Assign objects** task.
4. In the **Assignments** pane, select the assignment you want to change.
5. From the **Password Policies** menu, select the new password policy you want to apply.
6. Save the changes.

Editing password policies

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

To edit a password policy

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

Detailed information about this topic

- [General main data of password policies](#) on page 96
- [Policy settings](#) on page 96
- [Character classes for passwords](#) on page 98
- [Custom scripts for password requirements](#) on page 99

General main data of password policies

Enter the following main data of a password policy.

Table 21: main data for a password policy

Property	Meaning
Display name	Password policy name. Translate the given text using the  button.
Description	Text field for additional explanation. Translate the given text using the  button.
Error Message	Custom error message generated if the policy is not fulfilled. Translate the given text using the  button.
Owner (Application Role)	Application roles whose members can configure the password policies.
Default policy	Mark as default policy for passwords. This option cannot be changed. NOTE: The One Identity Manager password policy is marked as the default policy. This password policy is 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 22: Policy settings

Property	Meaning
Initial password	Initial password for newly created user accounts. The initial password is used if a password is not entered when you create a user account or if a random password is not

Property	Meaning
	generated.
Password confirmation	Reconfirm password.
Minimum Length	Minimum length of the password. Specify the number of characters a password must have. If the value is 0 , no password is required.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is 256 .
Max. errors	Maximum number of errors. Set the number of invalid passwords attempts. The number of failed logins is only taken into account when logging in to One Identity Manager. If the value is 0, the number of failed logins is not taken into account. This data is only taken into account if the One Identity Manager login was through a system user or employee based authentication module. If a user has exceeded the maximum number of failed logins, the employee or system user will not be able to log in to One Identity Manager. You can use the Password Reset Portal to reset the passwords of employees and system users who have been blocked. For more information, see the <i>One Identity Manager Web Designer Web Portal User Guide</i>.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires. If the value is 0 , then the password does not expire.
Password history	Enter the number of passwords to be saved. If, for example, a value of 5 is entered, the user's last five passwords are stored. If the value is 0 , then no passwords are stored in the password history.
Minimum password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value 0 means that the password strength is not tested. The values 1 , 2 , 3 and 4 specify the required complexity of the password. The value 1 represents the lowest requirements in terms of password strength. The value 4 requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted in the password. If this option is set, name properties are not permitted in passwords. The values of these columns are taken into account if the Contains name properties for

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

Character classes for passwords

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

Table 23: Character classes for passwords

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

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

Custom scripts for password requirements

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

Detailed information about this topic

- [Checking passwords with a script](#) on page 100
- [Generating passwords with a script](#) on page 101

Checking passwords with a script

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

Syntax of check scripts

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

With parameters:

policy = password policy object

spwd = password to check

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

Example: Script that checks a password

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

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

    Dim pwd = spwd.ToInsecureArray()
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            Throw New Exception(#LD("Password can't start with '?' or '!")#)
        End If
    End If
    If pwd.Length>2
        If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
            Throw New Exception(#LD("Invalid character sequence in password")#)
        End If
    End If
End Sub
```

To use a custom script for checking a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.

- a. In the Manager, select the **Oracle E-Business Suite > Basic configuration data > Password policies** category.
- b. In the result list, select the password policy.
- c. Select the **Change main data** task.
- d. On the **Scripts** tab, enter the name of the script to be used to check a password in the **Check script** field.
- e. Save the changes.

Related topics

- [Generating passwords with a script](#) on page 101

Generating passwords with a script

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

Syntax for generating script

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

With parameters:

policy = password policy object

spwd = generated password

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

Example: Script that generates a password

The script replaces invalid ? and ! characters at the beginning of random passwords with _.

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

    Dim pwd = spwd.ToInsecureArray()
    ' replace invalid characters at first position
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            spwd.SetAt(0, CChar("_"))
        End If
    End If
End Sub
```

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

To use a custom script for generating a password

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

Related topics

- [Checking passwords with a script](#) on page 100

Editing the excluded list for passwords

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

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

To add a term to the restricted list

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

Checking passwords

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

To verify if a password conforms to the password policy

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

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

Testing the generation of passwords

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

To generate a password that conforms to the password policy

1. In the Manager, select the **Oracle E-Business Suite > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Select the **Test** tab.
5. Click **Generate**.

This generates and displays a password.

Initial password for new E-Business Suite user accounts

You can issue an initial password for a new E-Business Suite user account in the following ways:

- When you create the user account, enter a password in the main data.
- Assign a randomly generated initial password to enter when you create user accounts.
 - In the Designer, set the **TargetSystem | EBS | Accounts | InitialRandomPassword** configuration parameter.

- Apply target system specific password policies and define the character sets that the password must contain.
- Specify which employee will receive the initial password by email.

Related topics

- [Password policies for E-Business Suite user accounts](#) on page 92
- [Email notifications about login data](#) on page 104

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 in a mail template is defined in several languages. This means the recipient's language can be taken into account when the email is generated. Mail templates are supplied in the default installation with which you can configure the notification procedure.

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

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

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

To send initial login data by email

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

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

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

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

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

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

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

Managing entitlement assignments

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

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

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

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

Table 24: Identification of direct and indirect entitlement assignments in EBSUserInResp table

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

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 more 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 107
- [Validity period of permission assignments](#) on page 117

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 a E-Business Suite user account, the entitlements are assigned to this user account.

Entitlements can also be assigned to employees through IT Shop requests. To enable the assignment of entitlements using 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. You can also group any number of company resources into a system role.

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

For detailed information see the following guides:

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

Detailed information about this topic

- [Validity period of permission assignments](#) on page 117
- [Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts](#) on page 108
- [Assigning E-Business Suite entitlements to departments, cost centers, and locations](#) on page 109
- [Assigning E-Business Suite entitlements to business roles](#) on page 111
- [Assigning E-Business Suite user accounts directly to an entitlement](#) on page 114
- [Adding E-Business Suite entitlements to system roles](#) on page 112
- [Adding E-Business Suite entitlements to the IT Shop](#) on page 112
- [Assigning E-Business Suite entitlements directly to a user account](#) on page 116

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

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

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

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

To configure assignments to roles of a role class

- a. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.
 - OR -
 - In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.
 - b. Select the **Configure role assignments** task and configure the permitted assignments.
 - To generally allow an assignment, enable the **Assignments allowed** column.
 - To allow direct assignment, enable the **Direct assignments permitted** column.
 - c. Save the changes.
2. Settings for assigning E-Business Suite entitlements to E-Business Suite user accounts.
 - E-Business Suite user accounts are labeled with the **Groups can be inherited** option.
 - E-Business Suite user accounts are linked with an employee through the UID_Person (**Person**) column.
 - E-Business Suite user accounts and E-Business Suite entitlements belong to the same E-Business Suitesystem.

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

Related topics

- [Entering main data of E-Business Suite user accounts](#) on page 131
- [General main data of E-Business Suite user accounts](#) on page 131
- [Entering main data of E-Business Suite entitlements](#) on page 139
- [General main data of an E-Business Suite entitlement](#) on page 139

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

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

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

1. In the Manager, select the **Oracle E-Business Suite > entitlements** category.
2. Select the entitlements in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
 - On the **Departments** tab, assign departments.
 - On the **Locations** tab, assign locations.
 - On the **Cost centers** tab, assign cost centers.

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

To remove an assignment

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

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

1. In the Manager, select the **Organizations > Departments** category.
 - OR -In the Manager, select the **Organizations > Cost centers** category.
 - OR -In the Manager, select the **Organizations > Locations** category.
2. Select the department, cost center or location in the result list.
3. Select the **Assign E-Business Suite entitlements** task.
4. In the **Add assignments** pane, assign the entitlements.

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

To remove an assignment

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

Related topics

- [Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts](#) on page 108
- [One Identity Manager users for managing Oracle E-Business Suite](#) on page 10

Assigning E-Business Suite entitlements to business roles

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

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

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

1. In the Manager, select the **Oracle E-Business Suite > entitlements** category.
2. Select the entitlements in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, select the role class and assign business roles.

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

To remove an assignment

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

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

1. In the Manager, select the **Business roles > <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign E-Business Suite entitlements** task.
4. In the **Add assignments** pane, assign the entitlements.

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

To remove an assignment

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

Related topics

- [Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts](#) on page 108
- [One Identity Manager users for managing Oracle E-Business Suite](#) on page 10

Adding E-Business Suite entitlements to system roles

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

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

NOTE: Groups with the **Only use in IT Shop** option 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. In the Manager, select the **Oracle E-Business Suite > entitlements** category.
2. Select the entitlements in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

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

To remove an assignment

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

Related topics

- [Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts](#) on page 108

Adding E-Business Suite entitlements to the IT Shop

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

- The permissions must be labeled with the **IT Shop** option.
- The permission must be assigned a service item.

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

- If you only want the permission to be assigned to employees through IT Shop requests, the permissions must also be labeled with the **Use only in IT Shop**

option. Direct assignment to hierarchical roles or user accounts is no longer permitted.

NOTE: With role-based login, the IT Shop administrators can assign permissions to IT Shop shelves. Target system administrators are not authorized to add permissions to IT Shop.

To add a permission to the IT Shop.

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

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

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

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

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

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

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

Related topics

- [General main data of an E-Business Suite entitlement](#) on page 139
- [Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts](#) on page 108
- [One Identity Manager users for managing Oracle E-Business Suite](#) on page 10

Assigning E-Business Suite user accounts directly to an entitlement

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

To assign an entitlement directly to user accounts

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

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

To assign the entitlement to a user account:

1. Click **Add**.
2. Select the user account from the **User account** 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 117

Related topics

- [Invalid entitlement assignments](#) on page 124

Assigning E-Business Suite entitlements directly to a user account

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

To assign entitlements directly to a user account

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

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

To assign an entitlement to the user account

1. Click **Add**.
2. Select the entitlement you want to assign from the **E-Business Suite Entitlement** 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 117

Related topics

- [Invalid entitlement assignments](#) on page 124
- [Adding E-Business Suite entitlements to the IT Shop](#) on page 112

Validity period of permission assignments

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

Table 25: 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 One Identity Manager.
Description	Text field for additional explanation.

Calculation of the effective validity period

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

Table 26: 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.

Type of assignment	Validity period
Inheritance by department, location, cost center, or business role (not an assignment request)	Unlimited only The date of the assignment is set as the first date of the validity.
Inheritance through dynamic role	Unlimited only The date of the assignment is set as the first date of the validity.
Inheritance by system role	Unlimited only The date of the assignment is set as the first date of the validity.

The effective assignment is controlled by a schedule.

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

Detailed information about this topic

- [Assigning E-Business Suite entitlements to user accounts in One Identity Manager](#) on page 107

Related topics

- [Invalid entitlement assignments](#) on page 124

Effectiveness of entitlement assignments

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

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

NOTE:

- You cannot define a pair of mutually exclusive entitlements. This means that the definition "Entitlement A excludes entitlement B" AND "Entitlement B excludes entitlement A" is not permitted.

- Each entitlement to be excluded from another entitlement must be declared separately. Exclusion definitions cannot be inherited.

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

Example of the effectiveness of entitlements

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

Clara Harris has a user account in this system. She primarily belongs to the "marketing" department. The "Control group" business role and the "Finance" department 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 an 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 27: Definition of excluded entitlements (EBSRespExclusion table)

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

Table 28: 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 "control group" business role 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 29: 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 **QER | Structures | Inherit | GroupExclusion** configuration parameter is set.

In the Designer, set the configuration parameter and compile the database.

NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

- Mutually exclusive entitlements belong to the same E-Business Suite system.

To exclude entitlements

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

- OR -

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

- Save the changes.

Related topics

- [Invalid entitlement assignments](#) on page 124

Inheritance of E-Business Suite entitlements based on categories

In One Identity Manager, user accounts can selectively inherit entitlements. To do this, entitlements, and user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the other tables, enter your categories for the permissions. Each table contains the category positions **position 1** to **position 63**.

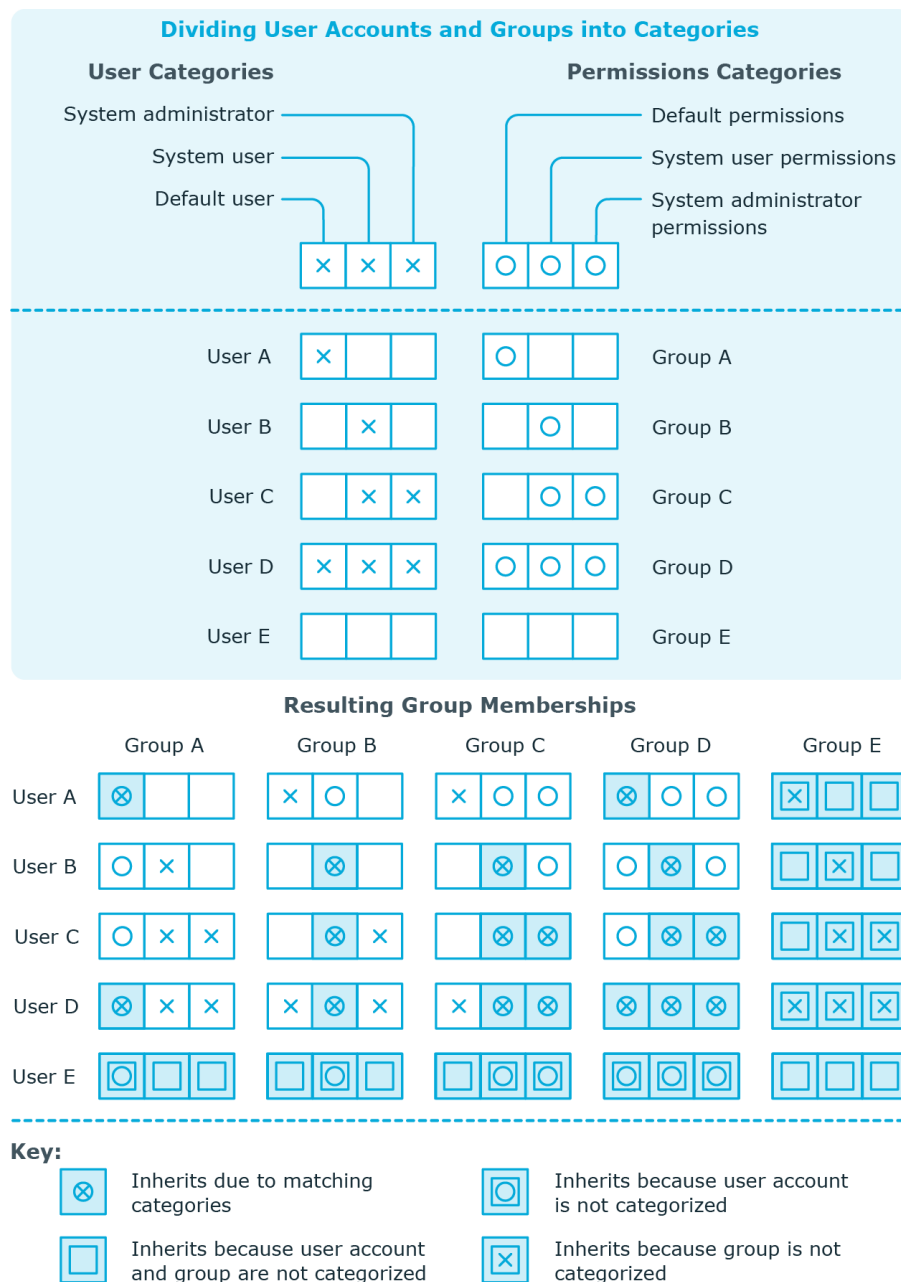
Every user account can be assigned to one or more categories. Each entitlement can also be assigned to one or more categories. If at least one of the category items between the user account and the assigned entitlement is the same, the entitlement is inherited by the user account. If the entitlement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

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

Table 30: Category examples

Category position	Categories for user accounts	Categories for permissions
1	Default user	Default entitlements
2	System users	System user entitlements
3	System administrator	System administrator entitlements

Figure 2: Example of inheriting through categories.



To use inheritance through categories

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

Related topics

- [Defining categories for the inheritance of E-Business Suite entitlements](#) on page 129
- [General main data of E-Business Suite user accounts](#) on page 131
- [General main data of an E-Business Suite entitlement](#) on page 139

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 through an account definition

For user accounts with the **Full managed** manage level, 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 by an account definition, the account definition defines how entitlement assignments are handled. If you do not want to retain the entitlement assignments, they are marked as invalid.

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

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

Related topics

- [Effectiveness of entitlement assignments](#) on page 119
- [Main data for manage levels](#) on page 64

- [Main data for account definitions](#) on page 60
- [Assigning E-Business Suite entitlements to departments, cost centers, and locations](#) on page 109
- [Assigning E-Business Suite entitlements to business roles](#) on page 111
- [Adding E-Business Suite entitlements to system roles](#) on page 112
- [Inheritance of E-Business Suite entitlements based on categories](#) on page 122

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.

Examples:

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

To display detailed information about assignments

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

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

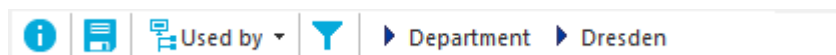


Table 31: Meaning of icons in the report toolbar

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 the E-Business Suite systems in the One Identity Manager database.

To set up a system:

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

General main data of E-Business Suite systems

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

Table 32: General main data of E-Business Suite systems

Property	Description
Display name	Name of the system to be displayed on the user interface
Account definition (initial)	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. User accounts are only linked to the employee (Linked) if no account definition is given. This is the case on initial synchronization, for example.
Target system managers	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. 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.
Synchronized by	Type of synchronization through which data is synchronized between the system and One Identity Manager. You can no longer change the synchronization type once objects for this system are present in One Identity Manager. When you create system using the Synchronization Editor, One Identity Manager is used.

Table 33: 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 74
- [Setting up account definitions](#) on page 59

- [Assigning employees automatically to E-Business Suite user accounts](#) on page 76
- [Target system managers](#) on page 163

Defining categories for the inheritance of E-Business Suite entitlements

In One Identity Manager, user accounts can selectively inherit entitlements. To do this, entitlements, and user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the other tables, enter your categories for the permissions. Each table contains the category positions **position 1** to **position 63**.

To define a category

1. In the Manager, select the system in the **Oracle E-Business Suite > Systems** category.
2. Select the **Change main data** task.
3. Switch to the **Mapping rule category** tab.
4. Extend the relevant roots of a table.
5. To enable the category, double-click .
6. Enter a category name of your choice for user accounts and entitlements in the login language that you use.
7. Save the changes.

Detailed information about this topic

- [Inheritance of E-Business Suite entitlements based on categories](#) on page 122

Editing the synchronization project for a E-Business Suite system

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

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

To open an existing synchronization project in the Synchronization Editor

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

Related topics

- [Customizing the synchronization configuration](#) on page 28

E-Business Suite user accounts

You use One Identity Manager to manage Oracle E-Business Suite user accounts. A user can log on to the E-Business Suite using their Oracle E-Business Suite user account. The user retains all permissions and security groups assigned to the user account. In addition, user accounts can also be linked to 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 main data described in the following is mapped through templates from employee main data.

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

Related topics

- [Managing E-Business Suite user accounts and employees](#) on page 58
- [Setting up account definitions](#) on page 59
- [Default project templates for synchronizing an Oracle E-Business Suite](#) on page 173
- [Entering main data of E-Business Suite user accounts](#) on page 131

Entering main data of E-Business Suite user accounts

To create a user account

1. In the Manager, select the **Oracle E-Business Suite > User accounts** category.
2. Click  in the result list.
3. On the main data form, edit the main data of the user account.
4. Save the changes.

To edit main data of a user account

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

Detailed information about this topic

- [General main data of E-Business Suite user accounts](#) on page 131
- [Login data for E-Business Suite user accounts](#) on page 135

General main data of E-Business Suite user accounts

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

Table 34: Additional main data of a user account

Property	Description
Employee	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. You can create a new employee for a user account with an identity of type Organizational identity, Personalized administrator identity, Sponsored identity, Shared identity, or Service identity. To do this, click  next to the input field and enter the required employee main data.

Property	Description
	Which login data is required depends on the selected identity type. 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.
Account definition	Account definition through which the user account was created. Use the account definition to automatically fill user account main data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account. NOTE: The account definition cannot be changed once the user account has been saved. NOTE: Use the user account's Remove account definition task to reset the user account to Linked status. This removes the account definition from both the user account and the employee. The user account remains but is not managed by the account definition anymore. The task only removes account definitions that are directly assigned (X0origin=1).
Manage level	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.
User name	User account identifier. If you have assigned an account definition, this input field is filled automatically depending on the manage level.
Display name	User account display name. If you have assigned an account definition, this input field is filled automatically depending on the manage level.
Distinguished name	User account's distinguished name. This is formed based on a template from the user name and the distinguished name of the E-Business Suite system.
Email address	User account email address. If you have assigned an account definition, this input field is filled automatically depending on the manage level.
Fax	Fax number for the user account. If you have assigned an account definition, this input field is filled automatically depending on the manage level.
Status	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)).

Property	Description						
	<table> <tr> <th>Status</th><th>Meaning</th></tr> <tr> <td>ACTIVE</td><td>The current date is within the validity period.</td></tr> <tr> <td>INACTIVE</td><td> - The active-from date has not yet been reached or the active-to date is in the past. - The user account has been deleted. </td></tr> </table>	Status	Meaning	ACTIVE	The current date is within the validity period.	INACTIVE	- The active-from date has not yet been reached or the active-to date is in the past. - The user account has been deleted.
Status	Meaning						
ACTIVE	The current date is within the validity period.						
INACTIVE	- The active-from date has not yet been reached or the active-to date is in the past. - The user account has been deleted.						
Active from (date)	First date from which the user account is valid. If you have assigned an account definition, this input field is filled automatically depending on the manage level. The template is only effective if the user account has been created as a new user account.						
Active to (date)	Last date from which the user account is valid. If you have assigned an account definition, this input field is filled automatically depending on the manage level.						
E-Business Suite system	E-Business Suite system in which you want to create the user account.						
Customer	Reference to an 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 set. For detailed information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .						
Category	Categories for the inheritance of E-Business Suite permissions to the user account. User accounts can selectively inherit permissions. To do this, entitlements, and user accounts are divided into categories. Select one or more categories from the menu.						

Property	Description
Description	Text field for additional explanation.
Identity	User account's identity type Permitted values are: • Primary identity: Employee's default user account. • Organizational identity: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • Personalized administrator identity: User account with administrative permissions, used by one employee. • Sponsored identity: User account to use for a specific purpose. Training, for example. • Shared identity: User account with administrative permissions, used by several employees. Assign all employees that use this user account. • Service identity: Service account.
Privileged user account.	Specifies whether this is a privileged user account.
Entitlements can be inherited	Specifies whether the user account may inherit E-Business Suite permissions through the employee. If this option is set, the user account inherits permissions through hierarchical roles or IT Shop requests. 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 E-Business Suite entitlement in the IT Shop. The request is approved and assigned. The user account only inherits this entitlement if this option is active.
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 by 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 58
- [Setting up account definitions](#) on page 59
- [Assigning employees automatically to E-Business Suite user accounts](#) on page 76
- [Inheritance of E-Business Suite entitlements based on categories](#) on page 122

- [Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts](#) on page 108
- [Disabling E-Business Suite user accounts](#) on page 137
- [Linking E-Business Suite user accounts to imported employees](#) on page 83
- [Supported user account types](#) on page 85

Login data for E-Business Suite user accounts

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

Table 35: Login data for a user account

Property	Description
Last login	Date of last login.
Password	Password for the user account. The employee's central password can be mapped to the user account password. For detailed information about an employee's central password, see <i>One Identity Manager Identity Management Base Module Administration Guide</i>. If you use a random generated initial password for the user accounts, it is automatically entered when a user account is created. The password is deleted from the database after publishing to the target system. NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password 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	Data of last password change.
Logins	Permitted number of logins.
Days	Validity period for the password.

Related topics

- [Initial password for new E-Business Suite user accounts](#) on page 103

Additional tasks for managing E-Business Suite user accounts

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

Task	Topic
Overview of E-Business Suite user accounts	Displaying the E-Business Suite user account overview on page 136
Assigning permissions	Assigning E-Business Suite entitlements directly to a user account on page 116
Assigning extended properties	Assigning extended properties to E-Business Suite user accounts on page 136
Synchronize object	Synchronizing single objects on page 52

Displaying the E-Business Suite user account overview

To obtain an overview of a user account

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

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

Assigning extended properties to E-Business Suite user accounts

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

To specify extended properties for a user account

1. In the Manager, select the **Oracle E-Business Suite > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

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

To remove an assignment

- Select the extended property and double-click .

5. Save the changes.

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

Disabling E-Business Suite 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 **Full managed** manage level are disabled depending on the account definition settings. For user accounts with a manage level, configure the required behavior using the template in the `EBSUser.EndDate` column.

Scenario:

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

Scenario:

User accounts not linked to employees.

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

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

To activate a user account

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

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

Related topics

- [Setting up account definitions](#) on page 59
- [Creating manage levels](#) on page 62
- [Deleting E-Business Suite user accounts](#) on page 138

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 through the result list or the menu bar, the user account is deactivated. However, it still physically exists. After confirmation of the security prompt, the status of the user account is set to **INACTIVE**. The current date is stored as the last validity date of the user account (**Active to (date)**).

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 account definition assignment is removed, the user account that was created from this account definition is disabled.

Related topics

- [Disabling E-Business Suite user accounts](#) on page 137

E-Business Suite permissions

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

Entering main data of E-Business Suite entitlements

To edit the main data of an entitlement:

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

Detailed information about this topic

- [General main data of an E-Business Suite entitlement](#) on page 139

General main data of an E-Business Suite entitlement

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

Table 36: General main data of an entitlement

Property	Description
E-Business Suite Responsibility	Responsibility for which the entitlement is to be created The responsibility must belong to the same E-Business Suite system as the security group.

Property	Description
Security group	Security group for which the entitlement is to be created. The security group must belong to the same E-Business Suite system as the responsibility.
Display name	Display name for the entitlement
Category	Categories for the inheritance of entitlements to user accounts. User accounts can selectively inherit permissions. To do this, entitlements, and user accounts are divided into categories. Select one or more categories from the menu.
Risk index	Value for evaluating the risk of assigning the entitlement to user accounts. Enter a value between 0 and 1 . This field is only visible if the QER CalculateRiskIndex configuration parameter is set. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Service item	Service item for requesting the entitlement through the IT Shop.
IT Shop	Specifies whether the entitlement can be requested through the IT Shop. This entitlement can be requested by your employees through the Web Portal and 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 122
- [Prerequisites for indirect assignment of E-Business Suite entitlements to E-Business Suite user accounts](#) on page 108
- [Adding E-Business Suite entitlements to the IT Shop](#) on page 112

Additional tasks for managing E-Business Suite entitlements

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

Task	Theme
Overview of E-Business	Displaying E-Business Suite entitlement overviews on page

Task	Theme
Suite entitlements	141
assign user accounts	Assigning E-Business Suite user accounts directly to an entitlement on page 114
Assigning extended properties	Assigning extended properties to E-Business Suite entitlements on page 141
Exclude E-Business Suite entitlements	Effectiveness of entitlement assignments on page 119
Assign system roles	Adding E-Business Suite entitlements to system roles on page 112
Assign business roles	Assigning E-Business Suite entitlements to business roles on page 111
Assign organizations	Assigning E-Business Suite entitlements to departments, cost centers, and locations on page 109
Add to IT Shop	Adding E-Business Suite entitlements to the IT Shop on page 112
Synchronize object	Synchronizing single objects on page 52

Displaying E-Business Suite entitlement overviews

To obtain an overview of permissions

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

Assigning extended properties to E-Business Suite entitlements

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

To specify extended properties for an entitlement

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

4. In the **Add assignments** pane, assign extended properties.

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

To remove an assignment

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

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

E-Business Suite applications

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

To display the properties of an application:

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

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

To obtain an overview of an application:

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

Related topics

- [Synchronizing single objects](#) on page 52

E-Business Suite menus

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

To display the properties of a menu:

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

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

To view an overview of a menu:

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

Related topics

- [Synchronizing single objects](#) on page 52

E-Business Suite data groups

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

To display the properties of a data group:

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

To obtain an overview of a data group:

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

Related topics

- [Synchronizing single objects](#) on page 52

E-Business Suite data group units

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

To display the properties of a data group unit:

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

To obtain an overview of a data group unit:

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

Related topics

- [Synchronizing single objects](#) on page 52

E-Business Suite request groups

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

To display the properties of a request group:

1. In the Manager, select the **Oracle E-Business Suite > Hierarchical view > <E-Business Suite System> > Applications > <Application> > Request groups** category.

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

To obtain an overview of a request group:

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

Related topics

- [Synchronizing single objects](#) on page 52

E-Business Suite security groups

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

To display the properties of a security group:

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

To obtain an overview of a security group:

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

Related topics

- [Synchronizing single objects](#) on page 52

E-Business Suite attributes

E-Business Suite Attributes further restrict the responsibilities of user accounts. For this purpose, attributes can be assigned both to user accounts and to responsibilities. Attributes

are defined for each E-Business Suite application. They are imported into the One Identity Manager database during synchronization. You cannot edit the properties.

To display the properties of an attribute:

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

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

To view an overview of an attribute

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

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

Related topics

- [Synchronizing single objects](#) on page 52

E-Business Suite responsibilities

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

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

Related topics

- [Synchronizing single objects](#) on page 52

Displaying main data of E-Business Suite responsibilities

To display the properties of a responsibility:

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

To obtain an overview of a responsibility:

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

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

Detailed information about this topic

- [General main data of E-Business Suite responsibilities](#) on page 147

General main data of E-Business Suite responsibilities

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

Table 37: General main data of a responsibility

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

Property	Description
(date)	
Valid to (date)	Last date on which the responsibility is valid When this date has passed, the responsibility is deactivated.
Description	Additional information about the responsibility.
Language	Language code of the language in which the responsibility is saved in Oracle E-Business Suite.
Application	Application in which the responsibility is valid.
Data group unit	Data group unit for which the responsibility applies.
Menu	Menu for which the responsibility applies
Process group	Request group for which the responsibility applies.
Version	Version in which the responsibility is available Possible value are: • 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. In the Manager, select the **Oracle E-Business Suite > HR people** category.
2. Select the employee in the result list.
3. Select the **Change main data** task.

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

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

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

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

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

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

You can maintain all other main data in the usual way. For more information about editing 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 83
- [General main data of E-Business Suite user accounts](#) on page 131
- [Setting up a synchronization project for employee data](#) on page 26
- [Project template for HR data](#) on page 174

Suppliers and contacts

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

To display the properties of a supplier:

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

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

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

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

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

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

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

You can maintain all other main data in the usual way. For more information about editing 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 83
- [General main data of E-Business Suite user accounts](#) on page 131
- [Setting up a synchronization project for organizational data](#) on page 27
- [Project template for CRM data](#) on page 175

Parties

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

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

To display the properties of a party:

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

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

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

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

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

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

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

You can maintain all other main data in the usual way. For more information about editing 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 83
- [General main data of E-Business Suite user accounts](#) on page 131
- [Setting up a synchronization project for organizational data](#) on page 27
- [Project template for OIM data](#) on page 175

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 **E-Business Suite HR** data source.

To display locations that originate from the HR data import:

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

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

To edit locked main data:

- Location
- Description
- Street
- City
- Country

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

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

Related topics

- [Setting up a synchronization project for employee data](#) on page 26
- [Project template for HR data](#) on page 174

Departments

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

To display departments that come from importing HR data

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

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

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

Related topics

- [Setting up a synchronization project for employee data](#) on page 26
- [Project template for HR data](#) on page 174
- [Configuring department synchronization](#) on page 35

Reports about E-Business Suite objects

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. The following reports are available for E-Business Suite systems.

Table 38: Data quality target system report

Report	Published for	Description
Show overview	User account	This report shows an overview of the user account and the assigned permissions.
Show overview including origin	User account	This report shows an overview of the user account and origin of the assigned permissions.
Show overview including history	User account	This report shows an overview of the user accounts including its history. Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	Entitlement	This report finds all roles containing employees who have the selected system entitlement.
Show overview	Entitlement	This report shows an overview of the system entitlement and its assignments.
Show overview including origin	Entitlement	This report shows an overview of the system entitlement and origin of the assigned user

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

Table 39: Additional reports for the target system

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

Report	Description
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 My One Identity Manager > Data quality analysis category.

Handling of E-Business Suite objects in the Web Portal

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

- Managing user accounts and employees

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

- Managing entitlement assignments

When an entitlement is assigned to an E-Business Suite shelf, the IT Shop entitlement can be requested by the customer in the Web Portal. The request undergoes a defined approval process. The entitlement is not assigned until it has been approved by an authorized 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 the Web Portal can assign E-Business Suite entitlements to the business roles for which they are responsible. The entitlements are inherited by all persons who are members of these business roles.

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

- Attestation

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

- Governance administration

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

- Risk assessment

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

- Reports and statistics

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

For more information about the named topics, see [Assigning E-Business Suite entitlements to user accounts in One Identity Manager](#) on page 107 and refer to the following guides:

- One Identity Manager Web Designer 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. 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 59.

- Password policy

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 92.

- Target system types

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

For more information, see [Post-processing outstanding objects](#) on page 53.

- Servers

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

For more information, see [Job server for E-Business Suite-specific process handling](#) on page 159.

- Target system managers

A default application role exists for the target system manager in One Identity Manager. Assign the employees who have permission 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 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 163.

Job server for E-Business Suite-specific process handling

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

- In the Designer, create an entry for the Job server in the **Base Data > Installation > Job server** category. For more information about this, see the *One Identity Manager Configuration Guide*.
- In the Manager, select an entry for the Job server in the **Oracle E-Business Suite > Basic configuration data > Server** category and edit the Job server main data.

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

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

Related topics

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

Editing E-Business Suite Job servers

To edit a Job server and its functions

1. In the Manager, select the **Oracle E-Business Suite > Basic configuration data > Server** category.
2. Select the Job server entry in the result list.
3. Select the **Change main data** task.
4. Edit the Job server's main data.

5. Select the **Assign server functions** task and specify server functionality.
6. Save the changes.

Detailed information about this topic

- [General main data of Job servers](#) on page 160
- [Specifying server functions](#) on page 162

General main data of Job servers

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

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

Table 40: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Syntax: <Name of servers>.<Fully qualified domain name>
Target system	Computer account target system.
Language	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The Server is cluster and Server belongs to cluster properties are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the Robocopy and rsync programs are supported.

Property	Meaning
	If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed with the Robocopy program between servers with a Windows operating system or with the rsync program between servers with a Linux operating system. If the operating systems of the source and destination servers differ, it is important that the right copy method is applied for successful replication. A copy method is chosen that supports both servers.
Copy process (target server)	Permitted copying methods that can be used when this server is the destination of a copy action.
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.
Executing server	Name of the executing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. The process steps are requested by the Job queue using this queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values Win32 , Windows , Linux , and Unix are permitted. If no value is specified, Win32 is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager	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 Job Queue Info program. For more 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. NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently running.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

Related topics

- [Specifying server functions](#) on page 162

Specifying server functions

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

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

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

Table 41: Permitted server functions

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

Server function	Remark
CSV script server	This 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 synchronizes the Oracle E-Business Suite target system.

Related topics

- [General main data of Job servers](#) on page 160

Target system managers

A default application role exists for the target system manager in One Identity Manager. Assign the employees who have permission 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 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 allocates employees to be target system administrators.
2. These target system administrators add employees to the default application role for target system managers.

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

3. Target system managers can authorize other 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 42: Default application roles for target system managers

User	Tasks
Target system managers	Target system managers must be assigned to the Target systems Oracle E-Business Suite or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects. • Edit password policies for the target system. • Prepare entitlements to add to the IT Shop. • Can add employees who have another identity than the Primary identity. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other 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 the Manager as a One Identity Manager administrator (**Base role | Administrators** application role)
2. Select the **One Identity Manager Administration > Target systems > Administrators** category.
3. Select the **Assign employees** task.
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 in to the Manager as a target system administrator (**Target systems | Administrators** application role).
2. Select the **One Identity Manager Administration > Target systems > Oracle E-Business Suite** category.

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

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

1. Log in to the Manager as a target system manager.
2. Select the **Oracle E-Business Suite > Systems** category.
3. Select the system in the result list.
4. Select the **Change main data** task.
5. On the **General** tab, select the application role in the **Target system manager** 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 Oracle E-Business Suite](#) on page 10
- [General main data of E-Business Suite systems](#) on page 127

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 43: Configuration parameters

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 this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the <i>One Identity Manager Configuration Guide</i>.
TargetSystem EBS Accounts	Parameter for configuring E-Business Suite user account data.
TargetSystem EBS Accounts InitialRandomPassword	Specifies whether a random password is generated when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem EBS Accounts InitialRandomPassword SendTo	Specifies to which 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	Mail template name that is sent to supply users with the login

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

Configuration parameter	Meaning
TargetSystem EBS PersonAutoFullsync	Mode for automatic employee assignment for user accounts that are added to or updated in the database by synchronization.
TargetSystem EBS PersonExcludeList	Listing of all user account without automatic employee assignment. Names are listed in a pipe () delimited list that is handled as a regular search pattern. Example: ADMINISTRATOR GUEST KRBTGT TSINTERNETUSER IUSR_.* IWAM_.* SU PPORT_.* . * \$

The following configuration parameters are also required.

Table 44: 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	Sender's default email address for sending automatically generated notifications. Syntax: sender@example.com Example: NoReply@company.com You can enter the sender's display name in addition to the email address. In this case, ensure that the email address is enclosed in chevrons (<>). Example: One Identity <NoReply@company.com>
DPR Journal LifeTime	This configuration parameter specifies the synchronization log's retention period (in days). Older logs are deleted from the database.

Configuration parameter	Meaning
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. If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the <i>One Identity Manager Configuration Guide</i>.
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	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.
QER Structures Inherit 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 this parameter require the database to be recompiled.

Permissions required for synchronizing with Oracle E-Business Suite

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

Table 45: Tables and views with select entitlements

Tables	Views
• 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_profile_options • applsys.fnd_profile_option_values • applsys.fnd_request_groups • applsys.fnd_resp_functions • applsys.fnd_responsibility • applsys.fnd_responsibility_tl • applsys.fnd_security_groups	• 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_responsibility# • applsys.fnd_responsibility_tl# • applsys.fnd_security_groups# • applsys.fnd_security_groups_tl# • applsys.fnd_user#

Tables**Views**

- applsys.fnd_security_groups_tl
- applsys.fnd_user
- apps.fnd_user_resp_groups_all
- apps.fnd_user_resp_groups_direct
- apps.fnd_user_resp_groups_indirect
- apps.fnd_usr_roles

Table 46: Stored procedures with run permissions**Stored procedures**

- apps.fnd_preference

This grants permissions for the following procedures.

- apps.fnd_preference.put
- apps.fnd_preference.remove

- apps.fnd_user_pkg

This grants permissions for the following procedures.

- apps.fnd_user_pkg.AddResp
- apps.fnd_user_pkg.change_user_name
- apps.fnd_user_pkg.changepassword
- apps.fnd_user_pkg.CreateUser
- apps.fnd_user_pkg.DelResp
- apps.fnd_user_pkg.DisableUser
- apps.fnd_user_pkg.UpdateUser
- apps.fnd_user_pkg.user_synch

Table 47: Tables with select permissions for synchronizing people data**Tables****Views**

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

Tables

- hr.per_jobs
- hr.per_org_structure_versions
- hr.per_org_structure_elements
- hr.per_roles
- hr.per_sec_profile_assignments
- hr.per_security_profiles

Views

- hr.per_org_structure_elements#
- hr.per_sec_profile_assignments#
- hr.per_security_profiles#

Table 48: Tables with run permissions for synchronizing employee data**Tables**

- apps.per_sec_profile_asg_api

Table 49: Tables with select entitlements for schema types that are created in the connector schema, but are not contained in the default mapping**Tables**

- applsys.fnd_request_group_units
- applsys.fnd_request_sets
- applsys.fnd_request_sets_tl
- applsys.fnd_user_preferences

Views

- applsys.fnd_request_group_units#
- applsys.fnd_request_sets#
- applsys.fnd_user_preferences#

Default project templates for synchronizing an Oracle E-Business Suite

A default project template ensures that all required information is added in One Identity Manager. This includes mappings, workflows, and the synchronization base object. If you do not use a default project template you must declare the synchronization base object in One Identity Manager yourself.

Use a default project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor.

Detailed information about this topic

- [Project template for user accounts and entitlements](#) on page 173
- [Project template for HR data](#) on page 174
- [Project template for CRM data](#) on page 175
- [Project template for OIM data](#) on page 175

Project template for user accounts and entitlements

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

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

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

Project template for HR data

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

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

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

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

Project template for CRM data

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

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

Schema type in the target system	Table in the One Identity Manager Schema
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 project template uses mappings for the following schema types.

Table 53: 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

Editing system objects

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

Table 54: Methods available for editing schema types

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

Schema type	Read	Paste	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 (HRPersonSecondaryLocation)	Yes	No	No	No
Department (HROrganization)	Yes	No	No	No
Secondary assignment: department (HRPersonInOrganization)	Yes	No	No	No

Example of a schema extension file

```
<?xml version="1.0" encoding="utf-8" ?>
<EBSF12>
<ObjectNames>
<Object SchemaName="UserInRESPDirect" ParentSchemaName="ORA-RESPDirect"
DisplayPattern="%vrtDistinguishedName%" IsReadOnly="false" UseDistinct="false">
  <ObjectKey>
    <Key Column="APPS.FND_USER_RESP_GROUPS_DIRECT.USER_ID" 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" View="FND_APPLICATION#" Schema="APPLSYS"
APK="" USN="" WhereClause="" JoinParentTable="FND_USER_RESP_GROUPS_DIRECT"
JoinParentColumn="APPS.FND_USER_RESP_GROUPS_DIRECT.RESPONSIBILITY_
APPLICATION_ID" JoinChildColumn="APPLSYS.FND_APPLICATION.APPLICATION_ID" >
    <PK Column="APPLSYS.FND_APPLICATION.APPLICATION_ID" />
  </Table>
</ObjectNames>
</EBSF12>
```

```

</Table>

<Table Name="FND_USER" View="FND_USER#" Schema="APPLSYS" APK="USER_ID"
USN="LAST_UPDATE_DATE" WhereClause="" JoinParentTable="FND_USER_RESP_
GROUPS_DIRECT" JoinParentColumn="APPS.FND_USER_RESP_GROUPS_DIRECT.USER_ID"
JoinChildColumn="APPLSYS.FND_USER.USER_ID" >

    <PK Column="USER_NAME" />

</Table>

<Table Name="FND_SECURITY_GROUPS" View="FND_SECURITY_GROUPS#"
Schema="APPLSYS" APK="SECURITY_GROUP_ID" USN="LAST_UPDATE_DATE"
WhereClause="" JoinParentTable="FND_USER_RESP_GROUPS_DIRECT"
JoinParentColumn="APPS.FND_USER_RESP_GROUPS_DIRECT.SECURITY_GROUP_ID"
JoinChildColumn="APPLSYS.FND_SECURITY_GROUPS.SECURITY_GROUP_ID" >

    <PK Column="SECURITY_GROUP_ID" />

</Table>

<Table Name="FND_RESPONSIBILITY" View="FND_RESPONSIBILITY#"
Schema="APPLSYS" APK="" USN="" WhereClause="" JoinParentTable="FND_USER_
RESP_GROUPS_DIRECT" JoinParentColumn="APPS.FND_USER_RESP_GROUPS_
DIRECT.RESPONSIBILITY_ID, APPS.FND_USER_RESP_GROUPS_DIRECT.RESPONSIBILITY_
APPLICATION_ID" JoinChildColumn="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_
ID, APPLSYS.FND_RESPONSIBILITY.APPLICATION_ID" >

    <PK Column="APPLSYS.FND_RESPONSIBILITY.RESPONSIBILITY_ID" />

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

</Table>
</Tables>
<Functions>
    <Insert>
        <Function Name="$ebsUserPackageName$.AddResp">
            <Parameter Name="username" PropertyName="APPLSYS.FND_USER.USER_
NAME" PropertyType="CHAR" Mandatory="TRUE" />
            <Parameter Name="resp_app" PropertyName="APPLSYS.FND_
APPLICATION.APPLICATION_SHORT_NAME" PropertyType="CHAR"
Mandatory="TRUE" />
            <Parameter Name="resp_key" PropertyName="APPLSYS.FND_
RESPONSIBILITY.RESPONSIBILITY_KEY" PropertyType="CHAR"
Mandatory="TRUE" />
            <Parameter Name="security_group" PropertyName="APPLSYS.FND_
SECURITY_GROUPS.SECURITY_GROUP_KEY" PropertyType="CHAR"
Mandatory="TRUE" />
        </Function>
    </Insert>
</Functions>

```

```

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

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

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

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

```

```

        <Parameter Name="resp_app" PropertyName="APPLSYS.FND_
        APPLICATION.APPLICATION_SHORT_NAME" PropertyType="CHAR"
        Mandatory="TRUE" />

        <Parameter Name="resp_key" PropertyName="APPLSYS.FND_
        RESPONSIBILITY.RESPONSIBILITY_KEY" PropertyType="CHAR"
        Mandatory="TRUE" />

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

    </Function>
</Delete>
</Functions>
</Object>
</ObjectNames>
</EBSF12>

```

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

Technical support resources

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

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

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

A

- account definition 59
 - add to IT Shop 71
 - assign automatically 70
 - assign to all employees 70
 - assign to business role 69
 - assign to cost center 69
 - assign to customers 74
 - assign to department 69
 - assign to employee 68, 71
 - assign to location 69
 - assign to system roles 71
 - assign to user account 82
 - create 60
 - delete 74
 - IT operating data 65-66
 - manage level 62
- application role
 - target system managers 163
- APPS user 16
- attribute 145, 147
- authorization assignment
 - direct 106, 114, 116
 - indirect 106
 - invalid 124

B

- base object 32, 47

C

- calculation schedule 50
 - deactivate 52
- category 129
- configuration parameter 11, 166
- connector schema
 - extend 37
- convert connection parameter 32
- customer 131, 150
 - account definition (initial) 74

D

- data group 143
- data group unit 144
- default user accounts 86
- department 152
- direction of synchronization
 - direction target system 22, 30
 - in the Manager 22

E

- email notification 104
- employee
 - assign user account 82
 - delete 84
- employee assignment
 - manual 79
 - remove 79
 - search criteria 78

- user account 83
- excluded attribute 147
- exclusion definition 119
- extended property
 - E-Business Suite permissions 141
 - user account 136

G

- group identity 87

H

- hierarchy filter 35
- HR employee 131, 148

I

- identity 85
- inheritance
 - category 122
- initialize system connection 36
- IT operating data
 - change 67
- IT Shop shelf
 - assign account definition 71
 - assign permissions 112

J

- Job server
 - edit 18, 159
 - load balancing 48
 - properties 160

L

- load balancing 48

- location 152
- log file 55
- login data 104

M

- menu 142
 - excluded 147

N

- NLog 55
- notification 104

O

- object
 - delete immediately 53
 - outstanding 53
 - publish 53
- outstanding object 53

P

- participant 131, 150
- password
 - initial 103-104
- password policy 92
 - assign 94
 - character sets 98
 - check password 102
 - conversion script 99, 101
 - default policy 94, 96
 - display name 96
 - edit 95
 - error message 96
 - excluded list 102

- failed logins 96
- generate password 103
- initial password 96
- name components 96
- password age 96
- password cycle 96
- password length 96
- password strength 96
- predefined 93
- test script 99-100
- permission
 - about IT Shop requests 139
 - add to IT Shop 112
 - assign business role 111
 - assign category 139
 - assign cost center 109
 - assign department 109
 - assign extended properties 141
 - assign location 109
 - assign responsibility 139
 - assign role 107
 - assign security group 139
 - assign system role 112
 - assign user account 107, 114
 - category 122
 - edit 139
 - edit assignment 114
 - effective 119
 - exclusion 119
 - inheriting through categories 129
 - inheriting through roles 107
 - inheriting through system roles 112
 - overview 141
 - overview of all assignments 125
 - remove assignment 114

- risk index 139
- validity period 117
- personalized admin identity 87
- process group 144
- project template 173
- provisioning
 - accelerate 48

R

- reset revision 55
- reset start up data 55
- responsibility 139, 147
 - validity 147
- revision filter 36
- risk assessment
 - permission 139
 - user account 131

S

- schema
 - changes 34
 - shrink 34
 - update 34
- schema extension 37
- schema type
 - add additionally 37
 - function definition 45
 - hierarchy 43
 - method definition 45
 - object definition 40
 - object key definition 41
 - parameter 46
 - primary key 43
 - table definition 41

- variable for language version 47
- scope 35
- security attribute 136, 145, 147
- security group 139, 145
- server function 162
- single object synchronization 47, 52
 - accelerate 48
- SQL statement 36
- start up configuration 32
- supplier 131, 149
- synchronization
 - accelerate 36
 - authorizations 15, 170
 - base object
 - create 31
 - calculation schedule 50
 - configure 22, 28
 - connection parameter 22, 28, 31
 - customize schema 28
 - different E-Business Suite
 - systems 31
 - employee data 26
 - extended schema 31
 - HR data 26
 - only changes 36
 - participant 27
 - prerequisite 13
 - prevent 52
 - scope 28
 - simulate 55
 - start 22, 50
 - supplier 27
 - synchronization project
 - create 22
 - target system schema 31
 - user 15
 - variable 28
 - variable set 31
 - workflow 22, 30
- synchronization analysis report 55
- synchronization configuration
 - customize 28, 30-31
- synchronization log 55
 - contents 28
 - create 28
 - display 51
- synchronization project
 - create 22
 - deactivate 52
 - edit 129
 - project template 173
- synchronization server 17
 - configure 17
 - edit 159
 - install 18
 - Job server 18
 - server function 162
 - system requirements 17
- synchronization user 16
- synchronization workflow
 - create 22, 30
- synchronize department 35
- synchronize single object 52
- system
 - account definition 127
 - application roles 10
 - category 122
 - edit 127
 - employee assignment 78
 - report 153

- specify category 129
- synchronization type 127
- target system manager 10, 163
- system connection
 - change 32
 - enabled variable set 33

T

- target system manager 163
 - specify 127
- target system synchronization 53
- template
 - IT operating data, modify 67

U

- use case 142
- user access for Oracle E-Business Suite 16
- user account 130
 - administrative user account 87-89
 - apply template 67
 - assign employee 76
 - assign extended properties 136
 - assign permissions 116
 - assigned employee 131
 - assigned permissions 153
 - category 122
 - connected 82
 - customer 131
 - data quality 153
 - deactivate 137-138
 - default user accounts 86
 - delete 138
 - delete employee 84

- edit authorization assignment 116
- employee assignment 83
- group identity 87
- HR employee 131
- identity 85, 89
- login data 135
- manage level 81
- overview 136
- participant 131
- password 103, 135
 - notification 104
- personalized admin identity 87
- privileged user account 85, 90
- remove authorization assignment 116
- risk index 131
- security attribute 136
- set up 131
- status 131
- supplier 131
- type 85-87, 90
- unused 153

V

- validity of permission assignments 117
- validity period 117
- variable set 32
 - active 33

W

- wrapper 16

X

- XOrigin 106, 124